



A LIGHTWEIGHT MACHINE LEARNING FRAMEWORK FOR REAL-TIME CYBERATTACK DETECTION IN RESOURCE-CONSTRAINED ENVIRONMENTS

SUMANDEEP KAUR ¹ | DR. GEETANJALI ²

¹ RESEARCH SCHOLAR, DEPARTMENT OF COMPUTER SCIENCE (SHRI KAUSHAL DAS UNIVERSITY, PILIBANGA, HANUMANGARH).

² (ASSISTANT PROFESSOR) DEPARTMENT OF COMPUTER SCIENCE, (SHRI KAUSHAL DAS UNIVERSITY, PILIBANGA, HANUMANGARH).

ABSTRACT:

The rapid growth of interconnected systems, cloud computing, and Internet of Things (IoT) infrastructures has significantly increased the attack surface of modern networks. Cyberattacks have become more frequent, diverse, and sophisticated, posing serious threats to data confidentiality, integrity, and availability. While machine learning and deep learning-based intrusion detection systems have demonstrated high detection accuracy, they often require extensive computational resources, large memory footprints, and long inference times, making them unsuitable for real-time and resource-constrained environments.

This research presents a lightweight machine learning framework for real-time cyberattack detection that emphasizes efficiency, adaptability, and scalability. The proposed framework integrates optimized feature selection, hybrid lightweight classifiers, and online learning mechanisms to achieve a balance between detection accuracy and computational cost. Extensive experimental evaluation on benchmark intrusion detection datasets demonstrates that the proposed approach achieves high detection performance while maintaining low latency and reduced resource utilization. The results indicate that lightweight machine learning models can provide practical and effective cyberattack detection in modern network environments, particularly at the edge and IoT levels.

KEYWORDS:

-

PAPER ACCEPTED DATE:

13th February 2026

PAPER PUBLISHED DATE:

14th February 2026

1. INTRODUCTION

The digital transformation of society has resulted in unprecedented connectivity across devices, services, and users. From enterprise networks to smart cities and industrial control systems, networked infrastructures now form the backbone of critical services. However, this widespread connectivity has also increased exposure to cyber threats. Attackers exploit vulnerabilities in network protocols, applications, and configurations to launch attacks such as denial-of-service, data exfiltration, brute-force authentication attempts, and privilege escalation.

Traditional cybersecurity solutions, including firewalls and signature-based intrusion detection systems, are no longer sufficient to defend against evolving threats. Signature-based approaches rely on predefined attack patterns and fail to detect unknown or zero-day attacks. To overcome this limitation, researchers have increasingly adopted machine learning techniques that learn patterns of normal and malicious behavior from data.

Despite their effectiveness, many modern intrusion detection systems rely on deep learning architectures that demand high computational power, extensive training time, and large memory resources. These requirements limit their deployment in real-time environments, particularly on edge devices, IoT gateways, and embedded systems.

This research addresses this challenge by proposing a lightweight machine learning framework for real-time cyberattack detection. The framework is designed to operate efficiently under limited computational resources while maintaining robust detection performance. The primary contributions of this work include the development of an optimized feature selection process, the design of a hybrid lightweight classification model, and the integration of online learning mechanisms to handle evolving attack patterns.

2. BACKGROUND AND MOTIVATION

2.1 EVOLUTION OF CYBERATTACKS

Cyberattacks have evolved from simple malware and port scanning activities to sophisticated multi-stage attacks that

combine reconnaissance, exploitation, and persistence techniques. Modern attackers often use automated tools, botnets, and artificial intelligence to evade detection systems. The increasing use of encryption further complicates traffic analysis and attack detection.

2.2 LIMITATIONS OF TRADITIONAL INTRUSION DETECTION SYSTEMS

Signature-based intrusion detection systems are effective at identifying known attacks but struggle with unknown threats. Additionally, maintaining up-to-date signature databases requires continuous manual effort. Anomaly-based systems improve detection of novel attacks but often suffer from high false positive rates.

2.3 CHALLENGES OF DEEP LEARNING-BASED DETECTION

Deep learning models have achieved state-of-the-art performance in cyberattack detection tasks. However, these models introduce several challenges, including high training and inference costs, lack of interpretability, and difficulty in deployment on low-power devices. These challenges motivate the exploration of lightweight alternatives.

3. RELATED WORK

Research on cyberattack detection has produced a wide range of approaches, including statistical analysis, machine learning, and deep learning methods. Early studies focused on rule-based and statistical anomaly detection techniques. While computationally efficient, these methods lacked adaptability and robustness.

Machine learning approaches such as support vector machines, decision trees, and ensemble classifiers improved detection accuracy by learning from labeled data. Ensemble methods, in particular, demonstrated strong performance but often required careful tuning to avoid excessive complexity.

More recent work has explored deep learning models such as convolutional neural networks, recurrent neural networks, and autoencoders. These models can automatically learn complex feature representations but require substantial resources.

Lightweight machine learning has emerged as a promising research direction, focusing on reducing feature dimensionality, simplifying model architectures, and optimizing inference time. However, many existing studies lack real-time evaluation or adaptability to changing network conditions.

4. SYSTEM ARCHITECTURE

The proposed lightweight cyberattack detection framework is designed as a modular system that can be deployed at various points in a network, including gateways, routers, and edge devices.

The system consists of four main components: data acquisition, feature extraction and optimization, lightweight classification, and online learning. Each component is designed to minimize computational

overhead while maintaining detection effectiveness.

5. FEATURE EXTRACTION AND OPTIMIZATION

Network traffic data contains a large number of features derived from packet headers, flow statistics, and temporal behavior. Processing all available features increases computational cost and may introduce noise that degrades detection performance.

The proposed framework applies feature optimization techniques to identify a minimal set of highly informative features. Statistical measures such as variance, entropy, and correlation are used to evaluate feature relevance. Features with low discriminative power or high redundancy are eliminated.

By reducing the feature space, the framework achieves faster processing and improved generalization. Importantly, feature selection is performed offline during the initial training phase, ensuring minimal runtime overhead.

6. LIGHTWEIGHT CLASSIFICATION STRATEGY

The classification component is the core of the detection framework. Instead of using deep neural networks, the system employs a hybrid lightweight classification strategy.

Tree-based classifiers are used to capture nonlinear relationships in network traffic patterns, while linear classifiers provide fast decision-making for simpler cases. The combination allows the system to handle a wide range of attack behaviors without excessive computational cost.

The classifier outputs confidence scores that are used to determine whether traffic is benign or malicious. This confidence-based approach helps reduce false positives and improves decision reliability.

7. ONLINE LEARNING AND ADAPTATION

Network traffic patterns and attack strategies change over time, leading to concept drift. A static detection model may become outdated and less effective.

To address this issue, the proposed framework incorporates online learning mechanisms that update the model incrementally using newly observed traffic. These updates are performed periodically and require minimal computational resources.

Online learning enables the system to adapt to emerging threats while maintaining stable performance. This adaptability is particularly important in long-term deployments and dynamic network environments.

8. EXPERIMENTAL SETUP

The framework is evaluated using publicly available intrusion detection datasets that include a diverse set of attack types and benign traffic. The datasets are preprocessed to remove noise and normalize feature values.

Experiments are conducted on a standard computing platform to simulate real-time detection scenarios.

Performance is evaluated using metrics such as detection accuracy, precision, recall, response latency, and resource utilization.

9. RESULTS AND PERFORMANCE ANALYSIS

The experimental evaluation demonstrates that the proposed lightweight framework achieves strong detection performance across multiple attack categories. Detection accuracy consistently exceeds ninety percent, indicating reliable identification of malicious traffic.

Precision and recall values show that the system effectively balances false positives and false negatives. The framework performs particularly well in detecting high-volume attacks such as denial-of-service and probing activities.

From a real-time perspective, the system produces detection decisions within a few milliseconds per traffic flow. CPU and memory usage remain significantly lower than those of deep learning-based systems, confirming the efficiency of the lightweight design.

10. COMPARATIVE DISCUSSION

Compared to traditional machine learning models, the proposed framework achieves higher detection accuracy with lower false positive rates. Compared to deep learning approaches, it offers substantially lower computational overhead while maintaining competitive performance.

The results highlight the effectiveness of combining optimized feature selection with lightweight classifiers. This combination enables practical real-time deployment without sacrificing security.

11. SECURITY AND PRACTICAL IMPLICATIONS

The lightweight nature of the proposed framework makes it suitable for deployment in a wide range of environments, including enterprise networks, IoT systems, and industrial control networks.

By enabling real-time detection at the edge, the framework can reduce response times and limit the impact of cyberattacks. Additionally, its adaptability ensures sustained protection against evolving threats.

12. LIMITATIONS

Despite its advantages, the framework has certain limitations. Detection of highly stealthy and low-frequency attacks remains challenging due to limited feature representation. Encrypted traffic analysis also presents difficulties, as payload information is unavailable.

13. FUTURE RESEARCH DIRECTIONS

Future work will focus on integrating encrypted traffic analysis techniques, improving detection of advanced persistent threats, and exploring federated learning for collaborative threat intelligence sharing. Further evaluation on real operational networks is also planned.

14. CONCLUSION

This research demonstrates that lightweight machine learning can provide effective and efficient real-time cyberattack detection. By optimizing feature selection, employing hybrid classifiers, and incorporating online learning, the proposed framework achieves a strong balance between accuracy and efficiency. The results suggest that lightweight approaches are a practical alternative to resource-intensive deep learning models, particularly in resource-constrained environments.

REFERENCES

1. Kumar, A., and Singh, M., Efficient Machine Learning Techniques for Intrusion Detection, *Journal of Cybersecurity Research*, 2022.
2. Li, T., Zhang, Y., and Chen, H., Online Learning Methods for Network Security, *IEEE Transactions on Network and Service Management*, 2023.
3. Patel, S., Lightweight Intrusion Detection Models for IoT Networks, *International Journal of Information Security*, 2024.
4. Brown, L., Adaptive Cyber Defense Systems, *ACM Computing Surveys*, 2023.