International Journal of Information Technologies and Systems Approach
Volume 19 • Issue 1 • January-December 2026

Design of Dynamic Network Security Defense Mechanism Driven by Light GBM

Yiyu Dai
https://orcid.org/0009-0008-9469-5873
Information Technology Development and Management Office, Huaqiao University, China

Junzheng Lu
https://orcid.org/0009-0004-0317-3000
Information Technology Development and Management Office, Huaqiao University, China

Zesen Li
https://orcid.org/0009-0000-8353-4224
Huaqiao University, China

Jiawei Li
https://orcid.org/0009-0005-9892-4707
Information Technology Development and Management Office, Huaqiao University, China

Yunxi Lu
https://orcid.org/0009-0006-3546-8182
Graduate School of Management, St. Petersburg State University, Russia
Received: October 4th, 2025 | **Accepted:** December 9th, 2025

ABSTRACT

In today's complex and ever-changing network security environment, traditional static detection methods struggle to cope with the rapid evolution of attack methods and the real-time processing requirements of large-scale data traffic. To address these challenges, this study proposes a dynamic network security defense mechanism based on the light gradient boosting machine. It combines model parameter optimization, online updating strategies, and inference-acceleration methods to construct an intrusion detection system that achieves both high accuracy and low latency. To verify performance, two public datasets, NSL-KDD and CIC-IDS2017, are employed. The results show that the proposed model achieves an accuracy of 96.2% and an F1 score of 93.9% on NSL-KDD, and an accuracy of 95.8% and an F1 score of 93.9% on CIC-IDS2017. Its overall performance outperforms mainstream models such as support vector machine, random forest, and deep neural network approaches.

KEYWORDS

Dynamic Network Defense, LightGBM, Intrusion Detection System, Network Security

INTRODUCTION

In the context of accelerating digitalization and networking, cyberspace is facing increasingly severe security threats (Admass et al., 2024; Hasan et al., 2023; Pour et al., 2023). Various new attack methods continue to emerge, including advanced persistent threats, zero-day attacks, cross-site scripting, and distributed denial of service attacks. Such threats make traditional rule-based static security defense systems gradually unable to cope with today's dynamic and complex attack environment (De Azambuja et al., 2023; Jada & Mayayise, 2024).

DOI: 10.4018/IJITSA.397341

Against this backdrop, building a dynamic defense mechanism with real-time response, intelligent threat identification, and adaptive adjustment capabilities has become a core issue to be addressed in the field of network security (Premkumar et al., 2022; Zhao, 2020). Unlike traditional static protection, dynamic defense is a proactive and adaptive security concept. Its core idea lies in continuously changing and adjusting defense strategies to increase attackers' attack costs and uncertainties. Representative theories in this field include Moving Target Defense and Adaptive Security Architecture (Wang et al., 2025). Both emphasize that defense systems should possess closed-loop capabilities (e.g., prediction, protection, detection, and response), thereby providing theoretical guidance for constructing truly effective defense systems.

In recent years, the continuous development of machine learning technologies has driven remarkable results in their applications in network security subfields such as intrusion detection systems, malicious traffic identification, and abnormal behavior monitoring (He et al., 2023; Pinto et al., 2023). Ensemble learning algorithms represented by gradient boosting decision trees (GBDT), a boosted ensemble of decision trees, have demonstrated advantages in various network traffic analysis tasks due to their strong feature modeling capabilities and good generalization performance (Louk & Tama, 2023; Mishra, 2022). Among them, light gradient boosting machine (LightGBM)—an efficient implementation of GBDT—has advantages such as fast training speed, low resource consumption, support for large-scale data, and native processing of categorical features. Thus, it has become an ideal choice for handling high-dimensional, sparse network data and improving detection efficiency (Wang et al., 2022).

However, most current studies based on LightGBM still focus on offline modeling and static feature classification. They lack in-depth integration with dynamic defense strategies. This gap limits LightGBM's contribution to real-time defense capabilities (Saied et al., 2023; Taha & Malebary, 2020).

To address this research gaps, the core innovative contribution of this study lies in designing and implementing a dynamic network security defense mechanism driven by LightGBM. The specific innovations are as follows:

- **Constructing a Closed-Loop Architecture Integrating the Concept of Dynamic Defense:** This study not only uses LightGBM for high-precision attack detection but also embeds it into a complete closed-loop architecture that includes multi-source data perception, adaptive feature engineering, real-time model inference, and dynamic response control, thus practicing the core idea of the adaptive security architecture.
- **Designing and Implementing an Online Update and Incremental Learning Strategy:** To cope with the continuous evolution of attack behaviors, this study introduces an online learning mechanism based on sliding windows and incremental fine-tuning, effectively alleviating the performance degradation often observed in traditional static models when facing new types of attacks.
- **Verifying the Feasibility of Integrating High-Efficiency Models Into Dynamic Defense Systems:** Through experiments, this study proves that the low-latency characteristics of LightGBM enable it to meet the strict real-time requirements of dynamic defense. This provides a solid engineering practice basis for constructing efficient, intelligent, and resilient network defense systems.

LITERATURE REVIEW

As network threats grow increasingly complex, traditional static intrusion detection methods based on rule matching can no longer meet security requirements in dynamic environments. In recent years, machine learning technologies have been widely applied in network security scenarios, demonstrating strong threat-identification capabilities, particularly in intrusion detection systems.