RADemics

# Real-Time Ensemble Learning Frameworks for Adaptive Detection of Evolving Persistent Cyber Threats

Sreejith Sreekandan Nair, Mainak Ghosh
LEADING FINANCIAL FIRM, GURU NANAK INSTITUTE OF HOTEL MANAGEMENT

# Real-Time Ensemble Learning Frameworks for Adaptive Detection of Evolving Persistent Cyber Threats

[1]Sreejith Sreekandan Nair, Independent Research Scholar, Leading Financial Firm, Dallas, Texas, USA. hisreenair@gmail.com

[2]Mainak Ghosh, Assistant Professor, Department of Computer Application, Guru Nanak Institute of Hotel Management, Kolkata, West Bengal, India. ghoshmainak252@gmail.com

## Abstract

Ensemble learning techniques have emerged as a powerful solution for real-time cyber threat detection, addressing the challenges posed by the dynamic and evolving nature of cyberattacks. This chapter explores the application of various ensemble models, such as bagging, boosting, and stacking, in detecting persistent and sophisticated cyber threats. Emphasizing the real-time detection capabilities, the chapter delves into performance benchmarking, optimization strategies, and the integration of multiple classifiers to enhance accuracy, reduce latency, and manage computational efficiency. Additionally, the chapter highlights the practical deployment of these models in complex cybersecurity environments, where rapid detection and response are critical. By combining supervised and unsupervised learning, hybrid stacking models are examined for their effectiveness in multi-class detection scenarios. Key challenges and solutions in applying ensemble models to real-time cybersecurity are also discussed, providing a comprehensive framework for researchers and practitioners to leverage in securing digital infrastructures.

**Keywords:** Ensemble Learning, Cyber Threat Detection, Real-Time Detection, Performance Benchmarking, Hybrid Models, Multi-Class Detection.

## Introduction

The rapid evolution of cyber threats has made traditional cybersecurity methods increasingly ineffective in addressing modern attack vectors [1]. As cybercriminals develop more sophisticated techniques, it becomes crucial for cybersecurity systems to evolve and incorporate advanced methods for detecting and mitigating threats [2,3]. Ensemble learning techniques have emerged as a promising solution, combining multiple models to enhance the accuracy and reliability of threat detection systems [4]. These techniques leverage the strengths of different machine learning algorithms to create a more powerful detection system, capable of identifying a wider range of threats while minimizing the risk of false positives [5,6]. The adoption of ensemble learning in cybersecurity has proven particularly beneficial in detecting persistent, evolving threats that often evade traditional detection methods [7,8].

Ensemble learning methods, such as bagging, boosting, and stacking, each offer unique advantages in the context of cyber threat detection [9]. Bagging techniques, such as Random Forests, focus on reducing variance by aggregating predictions from multiple models trained on

different subsets of the data [10-15]. This approach improves stability and robustness in the face of noisy or incomplete data, which was common in real-world cybersecurity environments [16]. Boosting techniques, including AdaBoost and Gradient Boosting, seek to enhance model performance by iteratively focusing on misclassified instances [17,18]. This iterative approach can improve detection accuracy, particularly for difficult-to-detect attack types [19]. Stacking, a more complex ensemble technique, combines the predictions of multiple models through a meta-learner, resulting in improved performance by exploiting the complementary strengths of various classifiers [20]. Together, these ensemble methods provide a robust framework for addressing the evolving nature of cyber threats [21].

One of the significant advantages of ensemble learning techniques was their ability to address the dynamic nature of cyber threats in real-time [22]. Cybersecurity systems must be capable of detecting and responding to attacks as occur, often with limited time and resources [23]. Real-time detection was essential to prevent damage and minimize downtime [24,25]. Ensemble learning models are particularly well-suited for this task, as can process large amounts of data rapidly while maintaining high levels of accuracy. The ability to provide real-time, accurate threat detection was one of the key reasons why ensemble learning techniques have become central to modern cybersecurity solutions.