Term Project - Topic Selection

Saraka Chris Kouame
Yad097

CS-5463-904-202520

The Role of High-Performance Computing in Enhancing Machine Learning for Phishing Detection

Phishing attacks remain a formidable cybersecurity threat, relentlessly evolving to outpace traditional detection methods. Machine learning (ML) has emerged as a critical countermeasure, enabling proactive and adaptive identification of phishing attempts. Yet, the computational demands of ML—particularly for processing vast datasets or achieving real-time detection—often constrain its effectiveness. High-performance computing (HPC) addresses this bottleneck, delivering the power needed to boost the speed, scalability, and efficiency of ML models.

This survey investigates the integration of HPC with ML to tackle phishing detection challenges, focusing on three key areas:

- **ML Implementations on HPC Architectures**: This section explores how HPC systems, such as GPUs and distributed clusters, enhance ML model performance, enabling faster training and inference for phishing detection.
- **Advanced HPC Tools and Technologies**: It examines cutting-edge tools and frameworks that optimize ML scalability and real-time processing, spotlighting their role in countering dynamic phishing threats.
- **Impact on Performance Metrics:** Drawing from case studies, this analysis quantifies HPC's contributions to speed, accuracy, and resource efficiency in ML-based phishing detection systems.

Through a comprehensive review of foundational works, recent journal articles, and conference papers, this survey synthesizes state-of-the-art advancements at the intersection of HPC and ML for cybersecurity. It elucidates how high-performance technologies transform phishing detection, offering insights into key innovations and charting promising directions for future research.