RADemics

Hybrid Machine Learning Models Combining Support Vector Machines and Deep Reinforcement Learning for Cyber Risk Profiling

Srinivasan M.L, S. Surender, S. Keerthana
RAJALAKSHMI INSTITUTE OF TECHNOLOGY, VELALAR COLLEGE OF ENGINEERING AND TECHNOLOGY, K.S.RANGASAMY COLLEGE OF TECHNOLOGY.

Hybrid Machine Learning Models Combining Support Vector Machines and Deep Reinforcement Learning for Cyber Risk Profiling

[1]Srinivasan M.L, Assistant Professor, Computer Science and Engineering, Rajalakshmi Institute of Technology, Kuthambakkam, Post, Chembarambakkam, srinivasan.m.l@ritchennai.edu.in

[2]S. Surender, Assistant Professor, Medical Electronics, Velalar College of Engineering and Technology, Thindal, Erode-12. surender774@gmail.com

[3]S. Keerthana, Assistant professor, Information Technology, K.S. Rangasamy college of Technology, Tiruchengode. keerthanas@ksrct.ac.in

Abstract

The increasing complexity of cyber threats necessitates the development of advanced machine learning models that can efficiently detect, assess, and mitigate risks in realtime. Traditional machine learning approaches often struggle with evolving attack patterns, while deep learning models require extensive training data and computational resources. This book chapter explores a novel hybrid machine learning architecture that integrates Support Vector Machines (SVM) and Deep Reinforcement Learning (DRL) for cyber risk profiling. The hybrid approach leverages SVM's superior classification capabilities and DRL's adaptive decisionmaking to enhance cyber defense mechanisms against sophisticated attacks. Key aspects such as model architecture, feature engineering, computational efficiency, realtime adaptability, and attack surface reduction are systematically analyzed., advanced optimization techniques, including feature selection, model compression, parallel processing, and hardware acceleration, are explored to ensure scalability and realtime applicability in cybersecurity environments. Experimental evaluations and comparative analysis with traditional models demonstrate the superior performance of the hybrid SVMDRL framework in terms of accuracy, adaptability, and computational efficiency. The findings provide a comprehensive foundation for the next generation of AIdriven cybersecurity models, addressing the challenges of threat detection, risk assessment, and proactive cyber defense strategies.

Keywords: Cyber Risk Profiling, Hybrid Machine Learning, Support Vector Machines, Deep Reinforcement Learning, Attack Surface Reduction, Cybersecurity Optimization

Introduction

The increasing sophistication of cyber threats necessitates advanced defensive mechanisms capable of real-time threat detection, risk assessment, and mitigation. Traditional machine learning (ML) models, such as Support Vector Machines (SVM), Decision Trees, and Bayesian Networks, have been widely adopted for cybersecurity applications, particularly for intrusion detection and malware classification. However, these models often suffer from limited adaptability to evolving threats and high dependency on static datasets, which restrict their effectiveness in dynamic cyber environments. On the other hand, deep learning techniques, including Deep Neural Networks (DNNs) and Convolutional Neural Networks (CNNs), have demonstrated superior performance in feature extraction and pattern recognition but are computationally expensive and require large amounts of labeled training data. These challenges highlight the need for hybrid learning architectures that combine different ML paradigms to enhance cyber risk profiling and defense mechanisms.

Hybrid machine learning models have emerged as a powerful approach to cybersecurity, leveraging the strengths of multiple learning techniques to improve detection accuracy, adaptability, and decision-making. In particular, the integration of Support Vector Machines (SVM) with Deep Reinforcement Learning (DRL) has shown promise in addressing the limitations of standalone models. SVM is known for its robust classification performance, particularly in high-dimensional spaces, making it an ideal choice for distinguishing between normal and malicious activities in cybersecurity datasets. DRL, on the other hand, enhances adaptive decision-making, enabling cybersecurity systems to dynamically respond to emerging threats based on learned policies. By combining SVM's precise classification capabilities with DRL's reinforcement-based optimization, the proposed hybrid model can effectively identify, assess, and mitigate cyber risks in real-time.

A critical challenge in cybersecurity is ensuring scalability and computational efficiency, particularly when dealing with large-scale and high-velocity network traffic. Traditional ML models often struggle with the real-time processing of vast amounts of security data, leading to delays in threat detection and response. Deep learning models, despite their high accuracy, require substantial computational resources, making them less feasible for resource-constrained environments such as IoT networks and cloud-based cybersecurity systems. The hybrid SVM-DRL architecture addresses these limitations by optimizing feature selection, reducing dimensionality, and implementing efficient parallel computing techniques. model compression strategies, such as quantization, pruning, and knowledge distillation, can further enhance the computational efficiency of hybrid models while maintaining high detection accuracy.