Artificial Intelligence in Cybersecurity for Risk Assessment and Transparent Threat Detection Frameworks

Edited by

K. Saravanan, Shantha Visalakshi U, Vamsi Krishna, Krishna Kumar L

RAD
Emics

Editors

Mr. K. Saravanan, Docter of Philosophy, Cloud Computing domain, Anna University, Chennai, India.

Vamsi Krishna chidipothu, PhD, finance, information security.

Dr Mrs Shantha Visalakshi U, Associate Professor, MCA Department, Ethiraj College for Women (Autonomous), Chennai, India

Dr. Krishna Kumar L

ISBN: 978-93-49552-02-9

DOI Registration Platform: Registered and indexed with CrossRef

DOIs for individual chapters and the book can be accessed at www.rademics.com

Bibliographic Information: This publication is indexed with CrossRef and registered for global citation and discoverability. Complete bibliographic metadata are available through CrossRef and on the Rademics website.

Publisher Address: Rademics Research Institute, Coimbatore, India.

Typesetting: Rademics Publishing Services.

Website: www.rademics.com

For production/safety compliance: info@rademics.com

Detailed Table of Contents

The increasing complexity and scale of cyber-physical systems have amplified the challenges associated with real-time cyber threat detection and mitigation. Traditional anomaly detection methods often struggle to capture the intricate dependencies and temporal dynamics of evolving cyber threats in large-scale networks. Graph Neural Networks (GNNs) have emerged as a powerful tool for modeling cyber threats; however, their scalability, computational efficiency, and real-time adaptability remain critical research challenges. This book chapter presents a comprehensive study on Graph-Based Risk Analysis using Graph Neural Networks (GNNs) and Temporal Graph Neural Networks (TGNNs) to map cyber threat propagation in large-scale networks. It explores key aspects such as dynamic graph representation, sequential modeling of attack patterns, and trade-offs between accuracy and computational efficiency in real-world cybersecurity applications, the scalability challenges of graph-based anomaly detection systems are analyzed, including computational complexity, memory constraints, and parallel processing limitations. Several optimization techniques, including graph sampling, model compression, and distributed graph learning, are discussed to enhance real-time threat detection performance. The chapter also highlights future research directions, such as federated graph learning for decentralized cybersecurity, adversarial robustness in GNNs, and energy-efficient architectures for large-scale threat monitoring. By addressing these challenges, this study provides a foundation for developing scalable, efficient, and resilient graph-based cyber risk assessment frameworks that can effectively combat emerging cyber threats in interconnected digital ecosystems.

AI-Enhanced Attack Graphs Using Markov Decision Processes for Proactive Threat Hunting and Risk Forecasting 107

Jagdish Makhijani, Yashwant Pathak, Soumya Bajpai

The increasing sophistication of cyber threats and the expanding attack surface of modern networks necessitate advanced methodologies for proactive risk assessment and threat mitigation. Traditional attack graphs provide a structured representation of potential attack paths but often struggle with scalability, adaptability, and real-time threat intelligence integration. To address these limitations, this chapter explores the integration of AI-enhanced attack graphs with Markov Decision Processes (MDPs) for proactive threat hunting and cyber risk forecasting. AI-driven techniques, including graph neural networks (GNNs), reinforcement learning, and Bayesian inference, are leveraged to enhance attack graph performance, automate risk assessment, and optimize cybersecurity decision-making. The incorporation of MDPs provides a probabilistic framework for modeling adversarial behavior, enabling predictive analytics for threat evolution and automated mitigation strategies, hybrid AI models improve attack graph scalability by integrating deep learning for pattern recognition, evolutionary algorithms for optimization, and federated learning for distributed security intelligence. The proposed framework shifts cybersecurity from reactive defense mechanisms to a proactive, adaptive, and intelligence-driven approach. Case studies and experimental evaluations demonstrate the efficacy of AI-enhanced attack graphs with MDPs in large-scale, dynamic environments, reinforcing their potential for real time cyber defense applications. This chapter contributes to advancing risk-aware cybersecurity strategies, fostering automation in cyber risk profiling, and enhancing resilience against emerging threats.

Fuzzy Logic and Evolutionary Computation for Adaptive Cyber Risk Management in Dynamic Cloud Environments 139

Nivedhitha. M, Sumitha Manoj, R. Sambath Kumar

The increasing complexity and dynamism of cloud environments have introduced significant cybersecurity challenges, necessitating advanced risk assessment methodologies capable of handling uncertainty and evolving threats. Traditional risk management frameworks often rely on static and rule-based mechanisms, which lack adaptability in dynamic cloud ecosystems. To address these limitations, this chapter explores the integration of fuzzy logic and evolutionary computation for adaptive cyber risk management in cloud environments. Fuzzy logic provides a powerful framework for modeling imprecise security parameters and uncertainty in threat landscapes, enabling more flexible and context-aware risk assessment. Meanwhile, evolutionary computation offers an adaptive mechanism to optimize cybersecurity strategies through heuristic learning and intelligent decision-making. The chapter presents a hybrid risk assessment framework that leverages fuzzy inference systems to quantify risk levels and evolutionary algorithms to dynamically optimize security controls, it examines the scalability of fuzzy-evolutionary approaches in large-scale cloud infrastructures and their effectiveness in mitigating real-time cyber threats, such as zero-day attacks, insider threats, and advanced persistent threats. The potential integration of explainable AI (XAI), deep learning, and quantum computing in enhancing fuzzy based risk assessment models is also discussed. This research contributes to the advancement of self-learning, adaptive cyber defense mechanisms capable of proactively mitigating risks in multicloud and hybrid-cloud environments. The proposed framework ensures improved threat intelligence, automated risk prioritization, and enhanced decision transparency, offering a robust solution for next-generation cloud security.

Convolutional and Transformer-Based Deep Learning Architectures for Real-Time Anomaly Detection in Network Traffic 170

Nalini Poornima Suresh, V. Vallinayagi, S. Nanthini

The rapid expansion of digital infrastructures has led to an unprecedented increase in cyber threats, necessitating advanced techniques for real-time anomaly detection in network traffic. Traditional rule-based and statistical methods often fail to detect sophisticated attacks due to their reliance on predefined signatures and limited adaptability to evolving threats. Deep learning has emerged as a promising alternative, leveraging data-driven approaches to enhance detection accuracy. Convolutional Neural Networks (CNNs) have demonstrated efficiency in extracting spatial-temporal patterns from network traffic, while Transformer-based architectures excel in capturing long-range dependencies and sequential anomalies. However, existing solutions face challenges related to scalability, computational overhead, imbalanced datasets, and adversarial robustness. This chapter provides a comprehensive analysis of CNN and Transformer-based deep learning architectures for real-time anomaly detection, highlighting their strengths, limitations, and practical deployment challenges. A hybrid approach integrating CNNs and Transformers is explored to enhance detection performance by combining local feature extraction with global sequence modeling. the role of synthetic data augmentation, adaptive learning techniques, and adversarial defense mechanisms in improving model generalization and resilience is examined. Future research directions focus on explainable AI, lightweight models for real-time applications, and self-supervised learning for mitigating data scarcity. The insights presented in this chapter contribute to the advancement of AI-driven cybersecurity solutions, enabling proactive threat detection and risk mitigation in dynamic network environments.

AI-Driven SIEM (Security Information and Event Management) Systems Using Long Short-Term Memory (LSTM) for Log-Based Threat Detection 200

Surbhi Choudhary, S. Kalaiarasi, A. Joshua Sundar Raja

The increasing sophistication of cyber threats necessitates the adoption of advanced techniques for real-time anomaly detection in Security Information and Event Management (SIEM) systems. Traditional rule-based and signature-based approaches are no longersufficient to address emerging attack vectors and the growing volume of security logs. This chapter explores the integration of Long Short-Term Memory (LSTM) networks into SIEM systems for log-based threat detection, highlighting their capacity to capture temporal dependencies and identify subtle patterns in sequential log data. Despite their effectiveness, challenges such as data privacy concerns, limited access to high-quality labeled datasets, and computational complexity remain. To overcome these obstacles, privacy-preserving data synthesis techniques, such as Generative Adversarial Networks (GANs) and differential privacy, are proposed to generate realistic, high-quality synthetic datasets for model training, ensuring data confidentiality and regulatory compliance. The chapter discusses the potential of LSTM-based SIEM systems in enhancing cybersecurity defenses, as well as ongoing research efforts to address the scalability, accuracy, and interpretability of AI-driven models. Key research gaps and future directions in the application of LSTM to SIEM are also presented. This work provides valuable insights into the development of next-generation AI-driven cybersecurity solutions that can dynamically adapt to the evolving threat landscape.

Generative Adversarial Networks (GANs) for Augmenting Cyber Threat Intelligence and Enhancing Detection of Evasive Malware 233

Krishna Kumar, Jothi .P, Senthil Kumar Dhandapani

The rapid expansion of digital infrastructures has led to an unprecedented increase in cyber threats, necessitating advanced techniques for real-time anomaly detection in network traffic. Traditional rule-based and statistical methods often fail to detect sophisticated attacks due to their reliance on predefined signatures and limited adaptability to evolving threats. Deep learning has emerged as a promising alternative, leveraging data-driven approaches to enhance detection accuracy. Convolutional Neural Networks (CNNs) have demonstrated efficiency in extracting spatial-temporal patterns from network traffic, while Transformer-based architectures excel in capturing long-range dependencies and sequential anomalies. However, existing solutions face challenges related to scalability, computational overhead, imbalanced datasets, and adversarial robustness. This chapter provides a comprehensive analysis of CNN and Transformer-based deep learning architectures for real-time anomaly detection, highlighting their strengths, limitations, and practical deployment challenges. A hybrid approach integrating CNNs and Transformers is explored to enhance detection performance by combining local feature extraction with global sequence modeling. the role of synthetic data augmentation, adaptive learning techniques, and adversarial defense mechanisms in improving model generalization and resilience is examined. Future research directions focus on explainable AI, lightweight models for real-time applications, and self-supervised learning for mitigating data scarcity. The insights presented in this chapter contribute to the advancement of AI-driven cybersecurity solutions, enabling proactive threat detection and risk mitigation in dynamic network environments.

Reinforcement Learning for Automated Intrusion Detection and Adaptive Defense in Zero-Day Attack Scenarios 263

Krishna Kumar, Aishwaryaa. L K, Pradeep. K K

The increasing sophistication of cyber threats, particularly zero-day attacks, necessitates the development of intelligent and adaptive security mechanisms capable of real-time threat detection and mitigation. Traditional intrusion detection and prevention systems (IDPS) rely on static rule sets and

representations, making them highly effective for Dark Web analysis and cybercrime prediction. This chapter explores the integration of transformer-based models in cyber threat intelligence workflows, emphasizing their ability to automate the identification of emerging threats, detect cybercriminal activities, and forecast evolving attack patterns. Key challenges, including data scarcity, adversarial linguistic variations, and ethical considerations in Dark Web monitoring, are analyzed alongside potential solutions leveraging AI-driven methodologies., the chapter discusses the implications of transformer-based threat intelligence frameworks for real time cybersecurity applications and future research directions aimed at enhancing cyber resilience. The insights presented contribute to the advancement of AI-driven cyber threat intelligence, enabling proactive threat mitigation strategies in an increasingly complex digital threat landscape.