

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, Doctor 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.

© 2025 RADemics Research Institute, Coimbatore, Tamil Nadu, India. 641 107

Publisher Address: Rademics Research Institute, Coimbatore, India.

Typesetting: Rademics Publishing Services.

Website: www.rademics.com

For production/safety compliance: info@rademics.com

All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without the prior written permission of the publisher.

Detailed Table of Contents

Bayesian Deep Learning for Probabilistic Risk Assessment and Attack Surface Reduction in Cyber Physical Systems 12

Er. Ram Prasad Pokhrel, B. Dineshkumar, Kayalvizhi K. R

CyberPhysical Systems (CPS) are increasingly targeted by sophisticated cyber threats, necessitating advanced Intrusion Detection Systems (IDS) capable of probabilistic risk assessment and adaptive defense mechanisms. Traditional deep learningbased IDS models, while effective in pattern recognition, lack uncertainty quantification, leading to unreliable classifications in dynamic attack environments. Bayesian Deep Learning (BDL) offers a principled approach to addressing this challenge by integrating probabilistic inference for enhanced threat detection and risk estimation. This book chapter explores the role of Bayesian Neural Networks (BNNs) in IDS, emphasizing their ability to model epistemic and aleatoric uncertainties, thereby improving detection accuracy and decision confidence. the chapter presents Bayesian Hyperparameter Optimization (BHO) as a scalable solution to optimize IDS model parameters, ensuring efficient and adaptive learning against evolving attack patterns. The integration of Bayesian techniques in both anomaly based and signature based IDS frameworks is examined, highlighting their potential in reducing false positives and mitigating adversarial attacks. , case studies and empirical evaluations are provided to demonstrate the real world applicability of BDL driven IDS in securing industrial control systems, smart grids, and IoT networks. The findings underscore the importance of uncertainty aware AI driven cybersecurity frameworks for robust and resilient CPS protection.

Hybrid Machine Learning Models Combining Support Vector Machines and Deep Reinforcement Learning for Cyber Risk Profiling 42

M.L, S. Surender, S. Keerthana

The increasing complexity of cyber threats necessitates the development of advanced machine learning models that can efficiently detect, assess, and mitigate risks in real time. 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 decision-making to enhance cyber defense mechanisms against sophisticated attacks. Key aspects such as model architecture, feature engineering, computational efficiency, real time 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 real-time applicability in cybersecurity environments. Experimental evaluations and comparative analysis with traditional models demonstrate the superior performance of the hybrid SVM-DRL framework in terms of accuracy, adaptability, and computational efficiency. The findings provide a comprehensive foundation for the next generation of AI driven cybersecurity models, addressing the challenges of threat detection, risk assessment, and proactive cyber defense strategies.

GraphBased Risk Analysis Using Graph Neural Networks for Mapping Cyber Threat Propagation in LargeScale Networks 72

S. Shanthi, Sathea Sree .S, M. Sindhu

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 107 Proactive Threat Hunting and Risk Forecasting

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 139 Management in Dynamic Cloud Environments

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 170 Real-Time Anomaly Detection in Network Traffic

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 200 Using Long Short-Term Memory (LSTM) for Log-Based Threat Detection

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 longer sufficient 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

signature-based techniques, which are insufficient against novel and evolving attack vectors. Reinforcement Learning (RL) offers a promising approach by enabling autonomous agents to learn optimal defense strategies through continuous interaction with network environments. This chapter explores the application of RL for automated intrusion detection and adaptive defense, focusing on its ability to enhance cyber resilience against zero-day attacks. It provides a comprehensive overview of RL-based threat detection frameworks, highlighting key methodologies such as Deep Q-Networks (DQN), actor-critic models, and deep reinforcement learning (DRL) architectures. The chapter examines the challenges associated with RL deployment in cybersecurity, including adversarial manipulation, computational complexity, and data scarcity, it discusses the integration of RL with security information and event management (SIEM) systems, real-time anomaly detection, and self-learning security policies. The proposed RL-driven approach enhances proactive threat hunting capabilities, minimizes false positives, and enables adaptive response mechanisms to emerging cyber threats. By leveraging RL techniques, cybersecurity frameworks can transition from reactive models to autonomous, self-evolving defense systems, ensuring enhanced protection in dynamic and adversarial environments.

Natural Language Processing-Based AI for Real-Time Phishing and Social Engineering Attack Detection in Email and Messaging Systems 292

Shruthi N, Suresh Kadarkarai, S. Nanthini

The increasing sophistication of phishing and social engineering attacks poses a significant threat to email and messaging security. Traditional rule-based and heuristic-driven approaches are often ineffective against evolving attack methodologies that exploit linguistic deception and psychological manipulation. Natural Language Processing (NLP)-based Artificial Intelligence (AI) has emerged as a powerful solution for real-time detection of phishing attempts by analyzing textual patterns, semantic structures, and contextual cues. However, deploying NLP-driven phishing detection in high-throughput email environments presents critical challenges, including scalability, concept drift, adversarial evasion, and multilingual attack vectors. This book chapter explores advanced NLP techniques, such as deep learning-based transformers, contextual embeddings, and hybrid AI models, for enhancing phishing and social engineering attack detection. It examines adaptive learning strategies to address concept drift, adversarial resilience mechanisms to counter evasive phishing tactics, and real-time processing architectures to ensure high-speed threat identification. Privacy-preserving AI frameworks and explainable NLP models are also discussed to enhance transparency and regulatory compliance in cybersecurity applications. By integrating state-of-the-art AI methodologies with real-time security monitoring, this chapter provides a comprehensive roadmap for developing robust, scalable, and intelligent phishing detection systems capable of mitigating emerging cyber threats in dynamic email and messaging ecosystems.

Transformer-Based Threat Intelligence Frameworks Using BERT and GPT 324 for Dark Web Analysis and Cybercrime Prediction

R. Boopathi, Indumathi Venkatesan, Briskilal. J

The increasing sophistication of cyber threats originating from the Dark Web has necessitated the development of advanced threat intelligence frameworks capable of detecting and predicting malicious activities in real time. Traditional cybersecurity approaches often struggle to process the vast, unstructured, and linguistically diverse data generated on underground forums and illicit marketplaces. Transformer-based natural language processing (NLP) models, such as Bidirectional Encoder Representations from Transformers (BERT) and Generative Pre-trained Transformers (GPT), have demonstrated exceptional capabilities in understanding and generating contextualized textual

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.

Explainable AI (XAI) for Cybersecurity Decision-Making Using SHAP and LIME for Transparent Threat Detection 354

Shantha Visalakshi Upendran, Karthiyayini. S, Dinesh Vijay Jamthe

The increasing complexity and sophistication of cyber threats have necessitated the integration of Explainable Artificial Intelligence (XAI) into cybersecurity frameworks to enhance transparency, trust, and decision-making. Traditional black-box machine learning models, despite their high accuracy, pose significant challenges in understanding threat detection mechanisms, leading to reduced interpretability and limited adoption in critical security applications. This book chapter explores the role of XAI techniques, specifically Shapley Additive Explanations (SHAP) and Local Interpretable Model-Agnostic Explanations (LIME), in improving the explainability of AI-driven cyber defense systems. A detailed analysis of computational efficiency, real-time applicability, and scalability challenges associated with SHAP and LIME in large-scale cybersecurity environments is provided., the chapter introduces hardware-accelerated approaches, such as FPGA-based optimization, to mitigate computational overhead while ensuring rapid and interpretable threat detection. reinforcement learning-based optimization for explainability is examined to enhance adaptive security mechanisms in dynamic threat landscapes. The integration of XAI-driven security information and event management (SIEM) systems is also discussed to bridge the gap between automated cyber threat detection and human-centric decision-making. This chapter provides a comprehensive exploration of state-of-the-art methodologies, challenges, and future research directions in the domain of XAI for cybersecurity, with a focus on balancing detection accuracy, computational efficiency, and interpretability.

Multi-Agent AI Systems for Coordinated Threat Response Using Deep Q-Networks (DQN) and Swarm Intelligence 387

Shantha Visalakshi Upendran, M R Mohanraj, Shiny Malar F. R

The increasing sophistication of cyber threats has made traditional defense mechanisms insufficient for addressing complex, large-scale attacks. Multi-Agent AI systems, particularly those utilizing Deep Q-Networks (DQN) and Swarm Intelligence (SI), have emerged as promising solutions for coordinated threat response in dynamic and distributed environments. These systems allow multiple agents to autonomously detect, assess, and mitigate threats through decentralized decision-making, enhancing scalability and efficiency in cybersecurity. However, ensuring the robustness and adversarial resilience of these systems remains a critical challenge. This chapter explores the integration of reinforcement learning and bio-inspired algorithms to develop a resilient multi-agent defense framework capable of adapting to both known and unknown cyber threats. The study examines the potential of DQN for adaptive learning in cyber defense, the role of SI in facilitating cooperative agent behavior, and strategies for improving system resilience against adversarial manipulations. Performance evaluations

demonstrate the effectiveness of the proposed approach in real-world threat scenarios, offering a new paradigm for autonomous and scalable cyber defense systems. The chapter provides insights into optimizing multi-agent AI systems for proactive, robust, and efficient cybersecurity in large-scale networks.

Cyber Deception Strategies Using AI-Powered Honeypots and Generative Models for Attacker Behavior Profiling 423

R. Shobana, V. Pavithra, R. Baghia Laxmi

Cyber deception strategies, powered by artificial intelligence (AI), have emerged as a critical tool in defending against increasingly sophisticated cyber threats. This chapter explores the integration of AI-driven honeypots and generative models for enhancing cybersecurity defenses, with a particular focus on mitigating cloud supply chain attacks. Cloud environments, characterized by their complexity and interconnected nature, have become prime targets for cybercriminals seeking to exploit vulnerabilities in trusted vendor relationships. AI-powered honeypots simulate realistic decoy systems within cloud infrastructures, luring attackers into engaging with fake environments, thus providing valuable intelligence on attacker tactics, techniques, and procedures (TTPs). The use of generative models, such as Generative Adversarial Networks (GANs), further strengthens deception by generating dynamic and convincing cloud service interactions, complicating attackers' efforts to identify legitimate systems. By continuously adapting to attacker behavior, AI-driven deception frameworks can offer real-time detection, analysis, and mitigation of supply chain compromises. The chapter also highlights the role of AI in enhancing the capabilities of traditional cybersecurity tools, such as intrusion detection systems (IDS) and Security Information and Event Management (SIEM) platforms, by providing more accurate and timely threat intelligence. As cloud-based services continue to grow, the application of AI-driven honeypots and generative models is poised to become a fundamental aspect of proactive, scalable, and adaptive defense mechanisms against cloud supply chain attacks.

Federated Learning for Distributed Threat Intelligence Sharing Across Global Cybersecurity Networks 456

Sowmiya S M, Nachimuthu S, A. Narayana Rao

The rapid evolution of cyber threats necessitates innovative approaches to enhance global cybersecurity collaboration. Federated Learning (FL) has emerged as a decentralized machine learning paradigm that enables distributed threat intelligence sharing while maintaining data privacy and security. This chapter explores the application of FL for large-scale cybersecurity networks, addressing critical challenges in scalability, security, and communication efficiency. The focus is on optimizing secure aggregation techniques to enable efficient and privacy preserving model updates across heterogeneous and resource-constrained environments. Key solutions such as hierarchical aggregation, sparse model updates, and blockchain-based enhancements are discussed to mitigate the computational and communication overheads inherent in federated systems. The chapter investigates the integration of advanced cryptographic methods, including homomorphic encryption and differential privacy, to strengthen the security of federated networks against adversarial attacks. By leveraging FL's potential, organizations can share threat intelligence across global networks without compromising sensitive data, significantly improving real-time cyber threat detection and response. The chapter concludes by identifying future research directions for overcoming existing challenges and further optimizing federated models in cybersecurity.

Post-Quantum Cryptography and Quantum Machine Learning for 489 Resilient Encryption in AI-Driven Cybersecurity

Krishna Kumar, Sathea Sree.S, R. Baghia Laxmi

The rapid evolution of quantum computing poses a significant challenge to traditional encryption systems, with the potential to compromise the security of sensitive digital infrastructures. Post-Quantum Cryptography (PQC) has emerged as a vital field, aiming to develop encryption algorithms resilient to quantum attacks. Simultaneously, Quantum Machine Learning (QML) is revolutionizing the way machine learning models process data, offering new avenues for enhancing cybersecurity measures. This chapter explores the integration of PQC and QML to create robust, future-proof encryption systems capable of adapting to the evolving threat landscape. By examining hybrid models that combine the quantum resistance of PQC with the adaptability and efficiency of QML, this work highlights the potential for creating scalable and efficient cryptographic frameworks. The challenges and opportunities presented by the intersection of PQC and QML are discussed, with a focus on resource-constrained environments where computational power and memory are limited. Through this analysis, the chapter offers a comprehensive roadmap for advancing AI-driven, quantum-resistant cybersecurity solutions, addressing both theoretical advancements and practical implementation challenges.

Neural Cryptographic Protocols Using Secure Multi-Party Computation 519 (SMPC) for Encrypted Data Processing in AI-Driven Security System

Shivi Dixit, A. Ramamoorthy, K.B. Anusha

The integration of Secure Multi-Party Computation (SMPC) and neural cryptographic protocols presents a novel approach to safeguarding data privacy in AI-driven security systems. This chapter explores the synergistic potential of these two advanced technologies, focusing on their application in privacy-preserving computations for real-time, large-scale AI systems. SMPC ensures secure collaborative computation across multiple parties without revealing sensitive data, while neural cryptographic protocols leverage machine learning to generate adaptable and efficient encryption schemes. The chapter delves into the theoretical foundations of both protocols, examines their performance benchmarks, and highlights the challenges and opportunities of combining them in AI environments. Key topics include optimizing computational efficiency, addressing scalability issues, and enhancing adversarial resilience in encrypted AI systems. By investigating the practical implications and use cases in domains such as secure federated learning, anomaly detection, and secure cloud-based AI applications, this chapter provides a comprehensive analysis of the future potential of SMPC and neural cryptography in advancing secure AI technologies. The findings offer valuable insights into developing scalable, efficient, and robust privacy-preserving solutions for next-generation AI-driven security systems.