1. Record Nr. UNINA9911018961503321

Autore	Mohanty Sachi Nandan
Titolo	Protecting and Mitigating Against Cyber Threats : Deploying Artificial Intelligence and Machine Learning
Pubbl/distr/stampa	Newark : , : John Wiley & Sons, Incorporated, , 2025 ©2025
ISBN	1-394-30521-4 1-394-30519-2
Edizione	[1st ed.]
Descrizione fisica	1 online resource (561 pages)
Altri autori (Persone)	SatpathySuneeta YangMing ValiD. Khasim
Disciplina	005.8
Soggetti	Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Cover -- Series Page -- Title Page -- Copyright Page -- Contents -- Preface -- Part I: Foundations of AI &amp -- ML in Security -- Chapter 1 Foundations of AI and ML in Security -- Abbreviations -- 1.1 Introduction -- 1.1.1 The Convergence of AI and ML in Security -- 1.2 Understanding Security Attacks -- 1.2.1 Types of Attacks and Vulnerability -- 1.2.2 How Attacks Exploit Vulnerabilities -- 1.2.3 Real-World Examples of AI and ML for Security -- 1.3 Evolution of Information, Cyber Issues/Threats Attacks -- 1.3.1 Cyber Security Threats -- 1.3.2 The Most Prevalent Security Attacks -- 1.4 Machine Learning for Security and Vulnerability -- 1.4.1 Data Collection and Preprocessing -- 1.4.2 Feature Engineering for Security Attack Detection -- 1.5 Challenges and Future Directions -- 1.6 Summary -- References -- Chapter 2 Application of AI and ML in Threat Detection -- 2.1 Introduction -- 2.2 Foundation of AI and ML in Security -- 2.2.1 Definition and Concepts -- 2.2.2 Types of Artificial Intelligence -- 2.2.3 Algorithms and Models in Machine Learning -- 2.3 AI and ML in Applications in Threat Detection -- 2.3.1 Next-Generation Endpoint Protection -- 2.3.2 Endpoint Detection and Response (EDR) -- 2.4 AI/ML Based Network Intrusion Detection Systems (NIDS) -- 2.5 Threat

Intelligence and Predictive Analytics -- 2.6 Challenges and Considerations -- 2.7 Integration and Interoperability -- 2.8 Future Directions -- 2.9 Conclusion -- References -- Chapter 3 Artificial Intelligence and Machine Learning Applications in Threat Detection -- 3.1 Introduction -- 3.2 Foundations of Threat Detection -- 3.2.1 Traditional Threat Detection Methods -- 3.2.2 The Need for Advanced Technologies -- 3.3 Overview of AI and ML -- 3.3.1 Understanding Artificial Intelligence -- 3.3.2 Machine Learning Fundamentals -- 3.4 AI and ML Techniques for Threat Detection.
3.4.1 Supervised Learning and Unsupervised Learning -- 3.4.2 Deep Learning -- 3.5 Challenges and Solutions -- 3.5.1 Imbalanced Datasets -- 3.5.2 Ability and Interpretability -- 3.6 Future Trends and Innovations -- 3.6.1 Evolving Technologies -- 3.6.2 Ethical Considerations -- Conclusion -- References -- Part II: AI &amp -- ML Applications in Threat Detection -- Chapter 4 Comparison Study Between Different Machine Learning (ML) Models Integrated with a Network Intrusion Detection System (NIDS) -- 4.1 Introduction -- 4.2 Related Work -- 4.3 Methodology -- 4.3.1 Data Preprocessing -- 4.3.2 Data Splitting -- 4.3.3 Machine Learning Models -- 4.4 Proposed Model -- 4.5 Experimental Result -- 4.5.1 Performance Evaluation Metrics -- 4.5.2 Results of XGBoost Classifier -- 4.5.2.1 Confusion Matrix -- 4.5.2.2 Accuracy/Recall/Precision -- 4.5.2.3 ROC Curve -- 4.5.3 Results of ExtraTrees Classifier -- 4.5.3.1 Accuracy/Recall/Precision/ROC Curve -- 4.5.4 Comparison and Discussion -- 4.6 Conclusion and Future Work -- References -- Chapter 5 Applications of AI, Machine Learning and Deep Learning for Cyber Attack Detection -- 5.1 Introduction -- 5.1.1 Evolution of Cyber Threats and the Need for Advanced Solutions -- 5.1.2 Taxonomy of Cyber Attacks -- 5.2 Background -- 5.2.1 What is Cyber Security? -- 5.2.2 Cyber Security Systems -- 5.2.3 Ten Different Cyber Security Domains -- 5.3 Role of AI for Cyber Attack Detection -- 5.3.1 Machine Learning for Cyber Attack Detection -- 5.3.2 Deep Learning as a Game Changer in Cyber Attack Detection -- 5.4 Cyber Security Data Sources and Feature Engineering -- 5.4.1 Data Sources -- 5.4.2 Feature Engineering -- 5.5 Training Models for Anomaly Detection in Network Traffic -- 5.5.1 Supervised Learning Models -- 5.5.2 Unsupervised Learning Models -- 5.5.3 Deep Learning Models -- 5.5.4 Hybrid Models.
5.6 Case Study: The Use of AI and ML in Combating Cyber Attacks -- 5.6.1 Analysis: Company X's Strategy for Detecting Cyber Attacks -- 5.6.1.1 Implementation -- 5.6.1.2 Results -- 5.7 Challenges of Artificial Intelligence Applications in Cyber Threat Detection -- 5.8 Future Trends -- 5.9 Conclusion -- References -- Chapter 6 AI-Based Prioritization of Indicators of Intelligence in a Threat Intelligence Sharing Platform -- 6.1 Introduction -- 6.2 Related Work -- 6.3 Methodology -- 6.3.1 Brief Code Explanation -- 6.3.1.1 Bringing in Libraries and Modules -- 6.3.1.2 Parting the Dataset -- 6.3.1.3 Making and Preparing the Model -- 6.3.1.4 Assessing the Model -- 6.3.1.5 Saving the Prepared Model -- 6.3.1.6 Stacking the Prepared Model -- 6.3.1.7 Information Assortment and Preprocessing -- 6.3.1.8 Extricating Remarkable IP Locations -- 6.3.1.9 Creating Highlights for IP Locations -- 6.3.1.10 Stacking Highlights Information -- 6.3.1.11 Foreseeing Needs -- 6.3.1.12 Printing IP Locations and Needs -- 6.3.2 Explanation of the Code Step-By-Step -- 6.4 Proposed Model -- 6.4.1 Workflow Model -- 6.4.2 Decision Tree Machine Learning Model and Its Usage in this Study -- 6.5 Experimental Result/Result Analysis -- 6.6 Conclusion -- 6.6.1 High Level AI Calculations -- 6.6.2 Reconciliation of Regular Language Handling (NLP) Strategies -- 6.6.3 Interpretability

and Reasonableness -- 6.6.4 Taking Care of Information Changeability -- 6.6.5 Ill-Disposed Assault Recognition -- 6.6.6 Moral Contemplations -- References -- Chapter 7 Email Spam Classification Using Novel Fusion of Machine Learning and Feed Forward Neural Network Approaches -- 7.1 Introduction -- 7.2 Literature Review -- 7.3 Proposed Methodology -- 7.4 Experimentation and Results -- 7.4.1 Data Assortment -- 7.4.2 Applying ML Algorithms -- 7.4.3 Apply FFNN -- 7.4.4 Apply Stacking Ensemble of RF and FFNN.
7.4.5 Apply Voting Ensemble of RF and FFNN -- 7.4.6 Comparison of All Models -- 7.5 Conclusion -- References -- Chapter 8 Intrusion Detection in Wireless Networks Using Novel Classification Models -- 8.1 Introduction -- 8.2 Literature Review -- 8.3 Methodology -- 8.4 State of the Art -- 8.5 Result Analysis -- 8.6 Conclusion -- References -- Chapter 9 Detection and Proactive Prevention of Website Swindling Using Hybrid Machine Learning Model -- 9.1 Introduction -- 9.2 Related Literature Survey -- 9.3 Proposed Framework -- 9.3.1 Block Diagram -- 9.3.2 Flow Chart -- 9.4 Implementation -- 9.4.1 Random Forest -- 9.4.2 XGBoost -- 9.4.3 CATBoost -- 9.5 Result Analysis -- 9.6 Conclusion -- References -- Part III: Advanced Security Solutions &amp -- Case Studies -- Chapter 10 Securing the Future Networks: Blockchain-Based Threat Detection for Advanced Cyber Security -- 10.1 Introduction -- 10.1.1 Background and Evolution of Cybersecurity Threats -- 10.1.2 The Need for Advanced Threat Detection -- 10.1.3 Review of Blockchain Technology in Cybersecurity -- 10.2 Understanding Blockchain Technology -- 10.2.1 Basics of Blockchain -- 10.2.2 Decentralization and Security Features -- 10.2.3 Smart Contracts and their Role in Security -- 10.3 Challenges in Traditional Threat Detection -- 10.3.1 Evolving Nature of Cyber Threats -- 10.3.2 The Importance of Proactive Security Solutions -- 10.4 Integrating Blockchain into Cybersecurity -- 10.4.1 Using Blockchain as the Basis for Improved Security -- 10.4.2 Consensus Mechanisms and Trust -- 10.4.3 Decentralized Identity Management -- 10.5 Challenges and Considerations of Blockchain in Cybersecurity -- 10.5.1 Scalability Issues in Blockchain -- 10.5.2 Regulatory and Compliance Challenges -- 10.5.3 Balancing Transparency and Privacy -- 10.6 Future Trends and Innovations and Case Studies of Blockchain Technology.
10.6.1 Emerging Technologies in Blockchain-Based Security Cyber Security -- 10.6.2 Industry Initiatives and Collaborations on Blockchain for Cybersecurity Solutions -- 10.7 Conclusion -- References -- Chapter 11 Mitigating Pollution Attacks in Network Coding-Enabled Mobile Small Cells for Enhanced 5G Services in Rural Areas -- 11.1 Introduction -- 11.2 Literature Survey -- 11.3 Proposed Model -- 11.4 Results -- 11.5 Conclusion -- References -- Chapter 12 Enhancing Multi-Access Edge Computing Efficiency through Communal Network Selection -- 12.1 Introduction -- 12.2 Related Work -- 12.3 Existing System -- 12.4 Proposed System -- 12.5 Implementation -- 12.6 Results and Discussion -- 12.7 Conclusion -- 12.8 Future Scope -- References -- Chapter 13 Enhancing Cyber-Security and Network Security Through Advanced Video Data Summarization Techniques -- 13.1 Introduction -- 13.1.1 Overview of Video Summarization -- 13.1.2 Importance of Efficient Video Management -- 13.2 Video Summarization Techniques -- 13.2.1 Clustering-Based Methods -- 13.2.2 Deep Learning Frameworks -- 13.2.3 Multimodal Integration Strategies (Audio, Visual, Textual) -- 13.3 Notable Advanced Techniques -- 13.3.1 SVS_MCO Method and Performance -- 13.3.2 Knowledge Distillation (KDAN Framework) -- 13.3.3 Advanced Models (Query-Based, Audio-Visual Recurrent Networks) -- 13.4 Graph-Based and Unsupervised Summarization -- 13.4.1 Graph-Based

Summarization Techniques -- 13.4.2 Unsupervised Summarization Methods (Two- Stream Approach for Motion and Visual Features) -- 13.5 Secure and Multi-Video Summarization -- 13.5.1 Secure Video Summarization -- 13.5.2 Multi-Video Summarization -- 13.6 Advanced Scene and Activity-Based Summarization -- 13.6.1 Scene Summarization -- 13.6.2 Activity Recognition -- 13.7 Performance Benchmarking and Evaluation.
13.7.1 Datasets and Evaluation Metrics (e.g., SumMe, TVSum).

Sommario/riassunto

The book provides invaluable insights into the transformative role of AI and ML in security, offering essential strategies and real-world applications to effectively navigate the complex landscape of today's cyber threats. Protecting and Mitigating Against Cyber Threats delves into the dynamic junction of artificial intelligence (AI) and machine learning (ML) within the domain of security solicitations. Through an exploration of the revolutionary possibilities of AI and ML technologies, this book seeks to disentangle the intricacies of today's security concerns. There is a fundamental shift in the security soliciting landscape, driven by the extraordinary expansion of data and the constant evolution of cyber threat complexity. This shift calls for a novel strategy, and AI and ML show great promise for strengthening digital defenses. This volume offers a thorough examination, breaking down the concepts and real-world uses of this cutting-edge technology by integrating knowledge from cybersecurity, computer science, and related topics. It bridges the gap between theory and application by looking at real-world case studies and providing useful examples. Protecting and Mitigating Against Cyber Threats provides a roadmap for navigating the changing threat landscape by explaining the current state of AI and ML in security solicitations and projecting forthcoming developments, bringing readers through the unexplored realms of AI and ML applications in protecting digital ecosystems, as the need for efficient security solutions grows. It is a pertinent addition to the multi-disciplinary discussion influencing cybersecurity and digital resilience in the future. Readers will find in this book: - Provides comprehensive coverage on various aspects of security solicitations, ranging from theoretical foundations to practical applications; - Includes real-world case studies and examples to illustrate how AI and machine learning technologies are currently utilized in security solicitations; - Explores and discusses emerging trends at the intersection of AI, machine learning, and security solicitations, including topics like threat detection, fraud prevention, risk analysis, and more; - Highlights the growing importance of AI and machine learning in security contexts and discusses the demand for knowledge in this area. Audience Cybersecurity professionals, researchers, academics, industry professionals, technology enthusiasts, policymakers, and strategists interested in the dynamic intersection of artificial intelligence (AI), machine learning (ML), and cybersecurity.