Machine Learning and Deep Learning Techniques for Cybersecurity Risk Prediction and Anomaly Detection

Chapter	Title	Page No.
1	Machine Learning Fundamentals for Intrusion Detection and Threat Classification	14
2	Deep Learning Concepts for Cyber Risk Prediction and Real Time Network Security	45
3	Data Collection Preprocessing and Feature Engineering for Cybersecurity Datasets	77
4	Supervised Learning Techniques for Malware Detection and Classification	109
5	Unsupervised Learning and Clustering Algorithms for Anomaly Detection in Network Traffic	138
6	Ensemble Learning Models for Improved Threat Prediction Accuracy	169
7	Adversarial Machine Learning in Cybersecurity Attacks and Defense Mechanisms	199
8	Convolutional Neural Networks for Cyber Threat Image Recognition and Payload Analysis	232
9	Recurrent Neural Networks and LSTM for Temporal Anomaly Detection in System Logs	263
10	Autoencoders for Unsupervised Intrusion Detection in High Dimensional Security Data	294
11	Transformer Models and Attention Mechanisms for Intelligent Cyber Threat Intelligence Extraction	325
12	Federated Learning and Edge AI for Privacy Preserving Cybersecurity Models	355
13	Hybrid AI Architectures Combining ML and DL for Insider Threat Detection	384
14	Reinforcement Learning for Adaptive Cyber Defense in Dynamic Threat Landscapes	416
15	Graph Neural Networks for Security Analysis of Complex Network Architectures	446

16	AI Based Security Solutions for Industrial Control Systems and SCADA Networks	474
17	Cybersecurity in IoT Ecosystems Using Lightweight Deep Learning Models	507