

Hybrid Machine Learning Techniques for Data Encryption, Anomaly Detection, and Zero-Day Attack Prevention

Chapter	Title	Page No.
1	Foundations of Hybrid Machine Learning Techniques in Cybersecurity for Robust Data Protection	12
2	Data Encryption Methodologies Enhanced by Hybrid Machine Learning Models for Secured Communication	38
3	Role of Feature Selection and Dimensionality Reduction in Hybrid Learning Systems for Threat Detection	66
4	Hybrid Supervised and Unsupervised Learning Models for Identifying Network Anomalies	92
5	Adaptive Machine Learning Algorithms for Real-Time Detection of Zero-Day Vulnerabilities	119
6	Neural Network Ensembles Combined with Statistical Models for Enhanced Encryption Algorithms	146
7	Evolutionary Computation and Deep Learning for Cryptographic Key Management and Security	172
8	Hybrid Clustering Techniques for Intrusion Detection in Multi-Layered Security Architectures	198
9	Support Vector Machines Integrated with Neural Networks for Cyber Threat Classification and Mitigation	225
10	Combining Rule-Based Systems with Machine Learning for Automated Anomaly Analysis	250
11	Reinforcement Learning Approaches Integrated with Hybrid Models for Proactive Threat Prevention	278
12	Ensemble Learning Frameworks for Improving the Accuracy of Zero-Day Exploit Detection	306
13	Federated Learning for Secure and Decentralized Anomaly Detection Across Networked Systems	333
14	Hybrid Models for Detecting Malware in Encrypted Traffic Using Behavioral Analysis	360
15	Application of Transfer Learning in Multi-Domain Hybrid Cybersecurity Solutions	385
16	Hybrid Deep Learning Architectures for Scalable Security in IoT and Edge Computing Environments	440