

## TABLE OF CONTENTS

Unit No.	Title	Page No.
1	<b>Introduction to Network Security and AI/ML Integration</b>	<b>1-17</b>
	1.1 Fundamentals of Network Security: Threats, Attacks, and Vulnerabilities 1.2 Importance of Real-Time Security Monitoring 1.3 Evolution of AI and ML in Cybersecurity 1.4 Key AI/ML Terminologies and Concepts 1.5 Role of AI/ML in Enhancing Network Security Posture	
2	<b>Data Collection, Preprocessing, and Feature Engineering for Network Security</b>	<b>18-41</b>
	2.1 Sources of Security Data: Logs, Network Traffic, IDS/IPS, SIEMs 2.2 Data Cleaning and Normalization Techniques 2.3 Labeling Network Attacks: Supervised vs Unsupervised Datasets 2.4 Feature Extraction from Network Packets 2.5 Dimensionality Reduction Techniques (PCA, t-SNE) 2.6 Handling Imbalanced and Noisy Security Datasets	
3	<b>Machine Learning Algorithms for Intrusion Detection Systems (IDS)</b>	<b>42-57</b>
	3.1 Classification Algorithms: Decision Trees, SVM, KNN, Naïve Bayes 3.2 Anomaly Detection vs Signature-Based Detection 3.3 Ensemble Methods: Random Forest, XGBoost for IDS 3.4 Evaluation Metrics: Accuracy, Precision, Recall, F1- Score, AUC 3.5 Real-Time IDS with Online Learning	
4	<b>Deep Learning Applications in Network Security</b>	<b>58-80</b>
	4.1 Deep Neural Networks (DNN) for Packet Classification 4.2 Convolutional Neural Networks (CNN) for Traffic Analysis 4.3 Recurrent Neural Networks (RNN, LSTM) for Time-Series Detection 4.4 Autoencoders for Anomaly and Malware Detection 4.5 Adversarial Attacks on DL Models and Defensive Strategies 4.6 Real-World Applications and Benchmarks	
5	<b>AI for Threat Intelligence and Behavioral Analytics</b>	<b>81-97</b>
	5.1 AI in Cyber Threat Intelligence: Indicators of Compromise (IoCs) 5.2 User and Entity Behavior Analytics (UEBA) 5.3 Clustering and Association Rule Mining for Threat Patterns 5.4 AI-driven Phishing Detection and Social Engineering Prevention 5.5 Visualization of Behavioral Anomalies	

<b>6</b>	<b>AI in Network Traffic Prediction and Security Automation</b>	<b>98-115</b>
	6.1 Forecasting Network Load to Prevent DDoS 6.2 AI-Driven Network Segmentation and Access Control 6.3 Self-Healing Networks and Automated Response Systems 6.4 Reinforcement Learning for Adaptive Security Policies 6.5 AI in SDN/NFV Security Management 6.6 Integration with Security Orchestration, Automation, and Response (SOAR)	
<b>7</b>	<b>Challenges, Ethics, and Future of AI in Network Security</b>	<b>116-135</b>
	7.1 Model Explainability and Interpretability in Cybersecurity 7.2 Adversarial Machine Learning: Poisoning and Evasion 7.3 Data Privacy, Security, and Compliance Challenges 7.4 AI Governance and Ethical Use in Network Defense 7.5 Future Trends: Federated Learning, Zero Trust with AI, Quantum Security 7.6 Capstone Project / Practical Assignment Guidance	