IV B.Tech I Semester

23A31702c	**AI IN CYBERSECURITY (Professional Elective-IV)**	**L**	**T**	**P**	**C**
		3	**0**	**0**	**3**

Course Objectives:

- To introduce the fundamental concepts of AI and their applications in cybersecurity.
- To understand AI-driven techniques for threat detection, classification, and mitigation.
- To explore machine learning and deep learning methods used for malware and intrusion detection.
- To equip students with skills in building intelligent security systems.
- To examine ethical, legal, and privacy aspects in AI-driven cybersecurity.

Course Outcomes:

- Understand AI principles and their relevance in cybersecurity.
- Apply machine learning techniques to detect and respond to threats.
- Analyze security incidents using intelligent tools and models.
- Evaluate and implement AI models for malware detection and anomaly analysis.
- Design AI-based cybersecurity frameworks for real-world scenarios.

UNIT I: Introduction to AI in Cybersecurity

Role of AI in Modern Cybersecurity, Overview of Cyber Threats and Attack Vectors, Fundamentals of Machine Learning for Security, AI vs Traditional Security Techniques, AI-Based Cyber Defense Lifecycle, Threat Intelligence with AI, Cybersecurity Data Types and Challenges, Case Studies of AI-Driven Attacks and Defenses

UNIT II: Machine Learning for Cyber Threat Detection

Supervised Learning for Intrusion Detection, Unsupervised Learning for Anomaly Detection, Feature Engineering from Network Traffic, Classification Algorithms: SVM, Decision Trees, Random Forests, Clustering Techniques: K-Means, DBSCAN, Ensemble Models and Model Evaluation Metrics, Real-Time Threat Detection Pipelines, Data Imbalance and Adversarial Sampling

UNIT III: Deep Learning in Cybersecurity

Neural Networks for Threat Classification, CNNs for Malware Detection from Binary Files, RNNs/LSTMs for Sequential Log Analysis, Autoencoders for Anomaly Detection,GANs in Malware Evasion and Defense,Transfer Learning for Threat Signature Extraction, Deep Learning vs Traditional Models: A Comparative Study,Real-World Use Cases and Limitations

UNIT IV: AI for Specific Security Domains

AI for Phishing and Spam Detection, AI in Cloud Security and Edge Devices, Botnet and DDoS Attack Detection**,** AI-Driven Endpoint Security, Natural Language Processing for Threat Intelligence, Behavioral Biometrics and Fraud Detection, AI in Social Engineering Attack Prevention, Security Information and Event Management (SIEM) with AI

UNIT V: Challenges, Ethics & Future of AI in Cybersecurity

Explainable AI (XAI) in Cybersecurity, Adversarial Attacks and Defenses in AI Systems, Data Privacy and Federated Learning, Legal and Ethical Issues in AI Security Solutions, AI Model Bias

and Fairness in Security Decisions, Securing AI Models Against Manipulation, Building Scalable AI-Powered SOCs, Future Trends: Autonomous Security, AI-Augmented Threat Hunting

Textbooks:

1. Clarence Chio & David Freeman, "Machine Learning and Security", O'Reilly Media.
2. Xiaofeng Chen et al., "Artificial Intelligence and Big Data Analytics for Cybersecurity", Springer.
3. Mark Stamp, "Information Security: Principles and Practice", Wiley.

Reference Books:

1. Sumeet Dua & Xian Du, "Data Mining and Machine Learning in Cybersecurity", CRC Press.
2. Shai Shalev-Shwartz & Shai Ben-David, "Understanding Machine Learning", Cambridge University Press.
3. Zhiwei Lin & Yang Xiang, "Cyber Security Intelligence and Analytics", Springer.
4. Bhavani Thuraisingham, "Data Mining for Malware Detection", CRC Press.

Online Learning Resources:

- Coursera – "AI for Cybersecurity" by University of Colorado
- Udemy – "Machine Learning for Cybersecurity"
- edX – "Cybersecurity MicroMasters" by RIT