18SN721 Essentials of Machine Learning for Cybersecurity 0-0-3

- Fundamentals of Machine Learning for Cyber Security.
- Supervised Learning- Linear Regression, Decisions Trees, Random Forests, SVM's, and Neural Networks.
- Anomaly Detection
- Unsupervised Learning- Dimensionality Reduction, PCA, T-SNE, Clustering, K-means
- Model Validation and Evaluation- Train Test Split, Cross Validation, Learning Curves, Model Complexity Curves, Overfitting vs Underfitting
- Security Issues in Machine Learning- Adversarial Attacks and Defenses, Privacy Attacks (differential privacy as defense)
- Lab-projects-Malware detection, Intrusion detection systems and Phishing detection

TEXTBOOKS/REFERENCES

Tom M Mitchell, Machine Learning, McGraw Hill, 1997