Tentatively Scheduled Lecture Session Plan

Machine Learning and its Application for Malware Analysis

19-30 September 2026 | Online Mode | 03:00-07:00 PM

10 lecture days x 4-hour session per day = 40 programme hours

Day 1 | Lecture 1: Malware and Cyber-Threat Landscape		Saturday, 19 September 2026
Module alignment: Module 1 - Introduction to Malware and Cyber Threat Landscape		
Session / Time	**Lecture Content**	**Faculty Name**
First Half 03:00-04:50 PM	Evolution of malware; major historical stages; changing attacker motives and capabilities. Malware taxonomy: viruses, worms, Trojans, ransomware, spyware and rootkits; representative examples.	**Dr. Ramesh Babu Battula**
04:50-05:00 PM Free Slot / Break		
Second Half 05:00-07:00 PM	Attack vectors and infection mechanisms: phishing, exploits, drive-by downloads, supply-chain and removable-media attacks. Malware kill chain and MITRE ATT&CK; framework; mapping a sample intrusion to tactics and techniques.	**Dr. Ramesh Babu Battula**

Day 2 | Lecture 2: Static Malware Analysis Fundamentals		Monday, 21 September 2026
Module alignment: Module 2 - Malware Analysis Fundamentals		
Session / Time	**Lecture Content**	**Faculty Name**
First Half 03:00-04:50 PM	Static versus dynamic malware analysis; safe laboratory workflow, sample handling and analysis objectives. Windows Portable Executable structure, headers, sections, imports, exports, strings and metadata.	**Dr. Smita Naval**
04:50-05:00 PM Free Slot / Break		
Second Half 05:00-07:00 PM	Tool-guided inspection using PE Studio, IDA Pro and Ghidra; control flow and suspicious-code indicators. Hands-on: static analysis of Windows PE malware samples and preparation of a concise findings report.	**Dr. Ramesh Babu Battula**

Day 3 | Lecture 3: Dynamic Analysis, Obfuscation and Sandboxing		Tuesday, 22 September 2026
Module alignment: Module 2 - Malware Analysis Fundamentals		
Session / Time	**Lecture Content**	**Faculty Name**
First Half 03:00-04:50 PM	Dynamic and behavioral analysis: processes, files, registry, persistence, system changes and indicators of compromise. Sandboxing principles and Cuckoo Sandbox workflow; interpreting behavioral and network reports.	**Dr. Smita Naval**
04:50-05:00 PM Free Slot / Break		
Second Half 05:00-07:00 PM	Malware obfuscation, packing and anti-analysis techniques; packer identification and unpacking indicators. Hands-on: behavioral analysis in a sandboxed environment and comparison with static-analysis findings.	**Prof. Vijay Laxmi**

Day 4 | Lecture 4: Feature Engineering and Machine Learning for Malware Detection		Wednesday, 23 September 2026
Module alignment: Module 3 - Feature Engineering for Malware Detection		
Session / Time	**Lecture Content**	**Faculty Name**
First Half 03:00-04:50 PM	Binary feature extraction: PE attributes, byte statistics, entropy, strings and structural metadata. Opcode analysis and n-gram features; vocabulary construction, frequency representations and dimensionality issues.	**Dr. Ramesh Babu Battula**
04:50-05:00 PM Free Slot / Break		
Second Half 05:00-07:00 PM	API-call and system-call features; sequence, frequency and behavioral representations. Network-traffic and behavioral features; hands-on feature extraction, dataset cleaning and preprocessing.	**Dr. Ramesh Babu Battula**

Lecture Session Plan (Continued)

Machine Learning and its Application for Malware Analysis

Day 5 | Lecture 5: Supervised Machine Learning for Malware Detection		Thursday, 24 September 2026
Module alignment: Module 4 - Machine Learning Techniques for Malware Detection		
Session / Time	**Lecture Content**	**Faculty Name**
First Half **03:00-04:50 PM**	End-to-end ML workflow: labels, train/validation/test splits, feature scaling, leakage prevention and class imbalance. Support Vector Machines and K-Nearest Neighbors for malware classification.	**Dr. Vikash Kumar**
04:50-05:00 PM Free Slot / Break		
Second Half **05:00-07:00 PM**	Random Forest and Naive Bayes models; feature importance and model interpretation. Hands-on: build, tune and compare supervised models on a malware dataset.	**Dr. Vikash Kumar**

Day 6 | Lecture 6: Unsupervised Learning and Performance Evaluation		Friday, 25 September 2026
Module alignment: Module 4 - Machine Learning Techniques for Malware Detection		
Session / Time	**Lecture Content**	**Faculty Name**
First Half **03:00-04:50 PM**	Clustering methods for malware family discovery and behavior-based grouping. Anomaly detection for novel and zero-day malware; assumptions, strengths and limitations.	**Dr. Abhinav Tomar**
04:50-05:00 PM Free Slot / Break		
Second Half **05:00-07:00 PM**	Evaluation metrics: confusion matrix, precision, recall, F1-score, ROC-AUC, PR-AUC and operational trade-offs. Hands-on: performance evaluation, threshold selection and comparison of supervised and unsupervised approaches.	**Dr. Vikash Kumar**

Day 7 | Lecture 7: Deep Learning for Advanced Malware Analysis		Saturday, 26 September 2026
Module alignment: Module 5 - Deep Learning for Advanced Malware Analysis		
Session / Time	**Lecture Content**	**Faculty Name**
First Half **03:00-04:50 PM**	Convolutional Neural Networks for malware image classification; binary-to-image representations. RNN and LSTM models for sequential API-call and system-call analysis.	**Dr. Abhinav Tomar**
04:50-05:00 PM Free Slot / Break		
Second Half **05:00-07:00 PM**	Autoencoders for anomaly detection and representation learning in malware datasets. Transfer learning and hands-on development of a neural-network malware classifier.	**Dr. Ramesh Babu Battula**

Day 8 | Lecture 8: Adversarial Malware, AI Security and Robustness		Monday, 28 September 2026
Module alignment: Module 6 - Adversarial Malware & AI Security		
Session / Time	**Lecture Content**	**Faculty Name**
First Half **03:00-04:50 PM**	Adversarial malware generation and evasion techniques against ML-based detectors. Case study: AI evasion attacks in real-world malware and their impact on detection pipelines.	**Dr. Ramesh Babu Battula**
04:50-05:00 PM Free Slot / Break		
Second Half **05:00-07:00 PM**	Training-data poisoning, backdoors and concept drift in evolving malware ecosystems. Secure and robust detection; federated malware learning under poisoning and adversarial-client attacks.	**Dr. Ramesh Babu Battula**

Lecture Session Plan (Continued)

Machine Learning and its Application for Malware Analysis

Day 9 | Lecture 9: Malware Detection in Mobile, IoT, Cloud and Edge		Tuesday, 29 September 2026
Module alignment: Module 7 - AI-Driven Malware Detection in Cloud, IoT & Mobile		
Session / Time	**Lecture Content**	**Faculty Name**
First Half **03:00-04:50 PM**	Android malware detection using AI; permissions, intents, API calls and hands-on Android dataset analysis. IoT malware, Mirai and botnets; hands-on extraction and analysis of IoT malware-traffic features.	**Dr. Ramesh Babu Battula**
04:50-05:00 PM Free Slot / Break		
Second Half **05:00-07:00 PM**	Cloud-based malware detection and Edge AI for low-latency, resource-aware malware defense. Federated learning for privacy-preserving and robust malware detection across IoT and edge devices.	**Dr. Ramesh Babu Battula**

Day 10 | Lecture 10: Integrated Applications and Research Directions		Wednesday, 30 September 2026
Module alignment: Module 7 - Integration, Open Research Challenges and Assessment		
Session / Time	**Lecture Content**	**Faculty Name**
First Half **03:00-04:50 PM**	Malware-analysis automation using AI; orchestration of static, dynamic and ML-assisted workflows. Threat intelligence and AI: indicator enrichment, campaign correlation and knowledge-driven detection.	**Dr. Ramesh Babu Battula**
04:50-05:00 PM Free Slot / Break		
Second Half **05:00-07:00 PM**	Open research challenges, reproducible experimentation, publication pathways and funding opportunities. Integrated case exercise, participant presentations, course review, assessment and feedback.	**Dr. Ramesh Babu Battula**

Schedule note: The programme runs on ten instructional days between 19 and 30 September 2026. Sundays, 20 and 27 September 2026, are excluded. Each session runs from 03:00 PM to 07:00 PM and includes a free slot from 04:50 PM to 05:00 PM.