Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(CS)

Field	Details
Course Name	Machine Learning Algorithms for Cyber Security
Course Code	CY-501
Semester	5
Course Category	Program Core Courses
Credits	3
Hours per Week	3L:0T:4P

1. Prerequisites

• Proficiency in Python programming (including libraries such as pandas, NumPy, and matplotlib)

• Fundamental knowledge of probability, statistics, and linear algebra (e.g., distributions, hypothesis testing, matrix operations)

• Basic understanding of computer networking and core security concepts (e.g., TCP/IP, CIA triad, cryptographic basics)

2. Course Learning Objectives

• This course introduces students to fundamental concepts and applications of the subject

• Students will learn theoretical foundations and practical skills relevant to the field

3. Teaching Methodology

• Lectures and Presentations

• Interactive Discussions and Case Studies

• Lab Sessions

• Guest Lectures

4. Evaluation System

Activities	Class Test Full Marks	Assignment Full Marks	Attendance Full Marks	Total Marks
CIA-1	25	10	05	40
CIA-2	25	10	05	40
End Semester Examination (ESE)	-	-	-	60
Total				100 Marks

5. Course Modules

Module	Topics	Hours
1	**Foundations of Cyber Security and Machine Learning** - Core security concepts (CIA triad, defense-in-depth, basic cryptography) - Overview of the cyber-threat landscape and common attacker motivations - Introduction to Artificial Intelligence and Machine Learning for security - Fundamental probability & statistics needed for ML (basic distributions, sampling, hypothesis testing) - Data acquisition, cleaning, exploratory visualization, and quality assessment - Feature extraction basics for security data (network logs, email headers, file metadata) - Python for data analysis - core libraries (pandas, NumPy, matplotlib) and scripting patterns	6
2	**Core Machine-Learning Techniques for Security** - Supervised learning fundamentals Linear & logistic regression Decision trees and random forests - Unsupervised learning fundamentals k-means and hierarchical clustering	8

	Simple anomaly-detection concepts - Feature engineering for security use-cases (malware binaries, network traffic, email) - Model evaluation & validation Accuracy, precision, recall, F1, ROC-AUC Cross-validation and basic statistical testing - Applied security tasks Spam & phishing detection Intrusion detection with SVM/decision-tree models Introductory malware classification pipeline	
3	**Deep Learning and Advanced Analytics in Cyber Security** - Neural-network basics Perceptron, multilayer perceptron, back-propagation - Convolutional Neural Networks (CNN) for security Image-based attacks, CAPTCHA solving, binary-image classification - Autoencoders for anomaly detection and feature compression - Dimensionality reduction & visualization Principal Component Analysis (PCA) t-SNE for security data exploration - Ensemble learning concepts Bagging & boosting (AdaBoost, Gradient Boosting) applied to security datasets - Time-series basics for DDoS and traffic anomaly detection Simple recurrent models (RNN/LSTM) and moving-average forecasting	7
4	**Threat Detection - Anomaly, Spam, and Intrusion** - Anomaly detection strategies Difference between supervised and unsupervised approaches Practical feature sets for network and host anomalies * Lab: build an auto-encoder-based anomaly detector - Spam & phishing detection workflow Text preprocessing, feature hashing, model training - Intrusion Detection Systems (IDS) Signature-based vs. behavior-based IDS Implementing an SVM-based network IDS	6

	- Consumer-web abuse mitigation Types of web abuse (credential stuffing, fake accounts) Supervised and clustering approaches to abuse detection	
5	**Advanced Security Applications - Malware, Network Traffic, Fraud, DDoS & Adversarial ML** - Malware analysis foundations Static vs. dynamic analysis, feature extraction from binaries - Network traffic analysis for threat detection Flow-based features, DGA detection, predictive attack classification - Financial fraud detection Credit-card transaction patterns, outlier detection models - DDoS detection using time-series methods Feature engineering for traffic bursts, simple LSTM model - Adversarial machine learning basics Common attacks (evasion, poisoning), model-stealing overview Defensive techniques (adversarial training, input sanitization) - Brief overview of online/streaming learning for malicious executable detection (conceptual only)	8
6	**Production, Deployment, and Ethical Considerations** - ML system maturity & scalability Data and model quality gates, versioning, CI/CD for ML - Monitoring, alerting, and reliability of ML pipelines Drift detection, performance dashboards, incident response - Ethical, legal, and privacy aspects Responsible AI, GDPR/CCPA implications, bias mitigation - Model robustness & defenses Practical adversarial defenses, privacy-preserving nearest-neighbor search - Course project workflow Proposal development, checkpoint reporting, final presentation & technical report - Benchmark datasets & case studies KDD-Cup 1999 (network traffic), Kaggle credit-card fraud, malware-family datasets	7

6. References

Textbooks:

1. Hands-On Machine Learning for Cybersecurity by Soma Halder and Sinan Ozdemir; Packt Publisher

2. Tom Mitchell. Machine Learning. McGraw Hill, 1997.

3. Gupta, Brij B., and Quan Z. Sheng, eds. Machine learning for computer and cyber security: principle, algorithms, and practices. CRC Press, 2019.

Reference Books:

1. Artificial Intelligence and Data Mining Approaches in Security Frameworks Editor(s):Neeraj Bhargava, Ritu Bhargava, Pramod Singh Rathore, Rashmi Agrawal, 2021.

2. Tsai, Jeffrey JP, and S. Yu Philip, eds. Machine learning in cyber trust: security, privacy, and reliability. Springer Science & Business Media, 2009.

3. Christopher M. Bishop. Pattern Recognition and Machine Learning. Springer 2006.

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
CY-501.1	Course Outcome 1	Understand	Understand
CY-501.2	Course Outcome 2	Understand	Understand
CY-501.3	Course Outcome 3	Understand	Understand
CY-501.4	Course Outcome 4	Understand	Understand
CY-501.5	Course Outcome 5	Understand	Understand
CY-501.6	Course Outcome 6	Understand	Understand

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	2	1	1	1	1	1	1	-	1	1	1	2
CO2	1	2	1	1	1	1	1	-	1	1	1	2

CO3	1	1	2	1	1	1	1	-	1	1	1	2
CO4	1	1	1	2	1	1	1	-	1	1	1	2
CO5	1	1	1	1	2	1	1	-	1	1	1	2
CO6	1	1	1	1	1	2	1	-	1	1	1	2

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	3	2	1
CO2	3	2	1
CO3	3	2	1
CO4	2	3	1
CO5	2	2	3
CO6	1	2	3

Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(CS)

Field	Details
Course Name	Introduction to Block Chain & Digital Forensics
Course Code	CY-502
Semester	5
Course Category	Program Core Courses
Credits	3
Hours per Week	3L:0T:0P

1. Prerequisites

• Fundamentals of computer networking (OSI model, TCP/IP, basic routing and switching)

• Basic operating-system concepts and command-line proficiency (Linux/Windows) with introductory scripting (e.g., Python or Bash)

• Introductory cybersecurity principles (CIA triad, risk management, basic cryptographic concepts)

2. Course Learning Objectives

• This course introduces students to fundamental concepts and applications of the subject

• Students will learn theoretical foundations and practical skills relevant to the field

3. Teaching Methodology

• Lectures and Presentations

• Interactive Discussions and Case Studies

• Lab Sessions

• Guest Lectures

4. Evaluation System

Activities	Class Test Full marks	Assignment Full marks	Attendance Full marks	Total Marks
CIA-1	25	10	05	40
CIA-2	25	10	05	40
End Semester Examination (ESE)	-	-	-	60
			Total	100 marks

5. Course Modules

Module	Topics	Hours
1	**Foundations of Cybercrime, Laws & Threat Landscape** - Definition and origins of cybercrime - Classification of cyber-crimes and typical threat actors - Information-security fundamentals (CIA triad, risk management basics) - Attack lifecycle overview (reconnaissance exploitation, post-exploitation) - Indian IT Act 2000 (key provisions & amendments) and brief overview of global frameworks (GDPR, ISO 27001) - Cyber-cafés and other public-access venues as enablers - Botnets and their role in large-scale attacks - Common attack vectors (phishing, drive-by, malicious links, insider threats) - Overview of tools and methods used in cybercrime (scanners, exploit kits, credential-dumping tools)	5
2	**Attack Techniques, Malware & Identity Threats** - Proxy servers, anonymizers and TOR basics - Password-cracking techniques (dictionary, rainbow tables, credential-spraying) - Keyloggers, spyware and basic anti-malware concepts - Malware families: viruses, worms, trojans, ransomware (principles & impact) - Steganography and covert data-hiding techniques	6

	- DoS and DDoS attack fundamentals and mitigation basics - Web-application attacks: SQL injection, XSS, CSRF - Buffer-overflow concepts and safe-coding reminders - Phishing, spear-phishing and social-engineering tactics - Identity theft - PII types, collection methods and protection strategies - Introduction to secure-coding practices	
3	**Network Defense & Intrusion Detection** - Firewall fundamentals (packet-filter vs. stateful inspection) - Stateless vs. stateful firewalls - when to use each - Packet characteristics used for filtering (IP, ports, protocols) - NAT, port-forwarding and basic network-address translation concepts - Configuring Linux iptables and Windows Firewall basics - VPN concepts - tunneling, encryption, common protocols (IPsec, SSL/TLS) - Intrusion Detection Systems - IDS vs. IPS, signature-based vs. anomaly-based - Snort introduction - rule syntax and simple deployment - Network-monitoring basics and log-analysis techniques - Security zones, DMZ design and host hardening - Introductory SIEM concepts (centralised log collection & correlation)	7
4	**Digital Forensics & Incident Response** - Need for cyber forensics and digital evidence handling - Digital-forensics life-cycle (identification, preservation, analysis, presentation) - Legal considerations, privacy issues and chain-of-custody requirements - Evidence sources and order of volatility hierarchy - Acquisition & duplication techniques for storage media and live systems - Imaging live systems, volatile memory collection and basic analysis tools - File-system and metadata analysis; recovery of deleted/hidden files - Email and messenger forensics - headers, attachments, chat logs - Mobile-device forensics (smartphones, tablets, wearables) - logical & physical extraction	8

	- Forensics of removable media (USB, SD cards, CDs/DVDs, cameras) - Structured incident-response process (preparation, detection, containment, eradication, recovery, lessons-learned) - Report writing, expert-witness testimony and evidence admissibility	
5	**Blockchain Fundamentals & Cryptographic Foundations** - Overview, history and definition of blockchain technology - Types of blockchains - public, private, permissioned - Core cryptographic primitives (hash functions, digital signatures, public-key cryptography) - Hash pointers, Merkle trees and their role in integrity verification - Block structure, transaction format and distributed ledger concepts - Basic consensus ideas (majority agreement, fault tolerance) - Smart-contract fundamentals and simple use-cases - Cryptocurrency basics - tokens, wallets and transaction flow - Security properties of blockchain (immutability, decentralization, resistance to tampering) - Practical cryptographic applications in security (password hashing, code signing, secure communication)	8
6	**Blockchain Consensus, Mining & Real-World Applications** - Bitcoin ecosystem: transaction lifecycle, double-spending protection, scripting basics - Mining process - block creation, propagation, difficulty adjustment, mining pools - Consensus mechanisms - conceptual overview of PoW, PoS, PBFT, and hybrid models (no heavy mathematics) - Forks and network upgrades - hard vs. soft forks, governance considerations - Permissioned/Private blockchains - Hyperledger Fabric, Corda architecture basics - Security and regulatory considerations for blockchain deployments - Real-world use-case spectrum: e-governance, land-registry, medical records, supply-chain, micropayments, IoT (e.g., IOTA), escrow services - Emerging trends - layer-2 scaling, tokenization, decentralized identity	8

6. References

Textbooks:

1. Artificial Intelligence and Blockchain in Digital Forensics Hardcover – 6 February 2023 by P. Karthikeyan (Editor), Hari Mohan Pande

2. Blockchain Technology, by Kumar Saurabh, Ashutosh Saxena, Wiley; First Edition (9 September 2020).

Reference Books:

1. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics by John Sammons, Syngress Media, U.S. (2 April 2012).

2. The Fundamentals Of Blockchain Technology by Saurabh Jain, Notion Press.

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
CY-502.1	Recall and list the key definitions, classifications, and legal provisions (Indian IT Act 2000, GDPR, ISO 27001) related to cybercrime, as well as the fundamental cryptographic primitives (hash functions, digital signatures, public-key cryptography).	Recall	Remember
CY-502.2	Explain the end-to-end attack lifecycle, major malware families, and the basic structure and consensus concepts of blockchain technology, illustrating how each relates to contemporary threat vectors.	Explain	Understand
CY-502.3	Implement firewall rules, configure a basic IDS/IPS (e.g., Snort), and apply secure-coding practices to mitigate at least three common web-application attacks (SQL injection, XSS, CSRF) in a lab environment.	Implement	Apply
CY-502.4	Analyze a simulated security incident by collecting volatile memory, imaging storage media,	Analyze	Analyze

	and using forensic tools to reconstruct the attack timeline, then produce a concise incident-response report following the structured IR process.		
CY-502.5	Evaluate the security properties, regulatory considerations, and potential vulnerabilities of different blockchain consensus mechanisms (PoW, PoS, PBFT) and smart-contract platforms, and recommend appropriate controls for a given use-case.	Evaluate	Evaluate
CY-502.6	Design an integrated cyber-security solution that combines traditional network defenses, forensic readiness, and blockchain-based integrity mechanisms to protect a specified organizational scenario, and justify the design choices with reference to best practices and legal requirements.	Design	Create

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	1	1	1	2	-	2	1	1	1	2
CO2	3	2	2	2	2	2	-	2	1	2	1	2
CO3	3	2	3	2	3	2	-	2	2	2	2	2
CO4	3	3	2	3	3	2	-	2	2	3	2	2
CO5	3	2	3	2	2	3	-	3	2	3	2	2
CO6	3	2	3	2	3	3	-	3	3	3	3	2

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	3	1	3
CO2	3	2	2
CO3	2	3	1
CO4	2	3	2
CO5	2	1	3
CO6	3	3	3

Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(AIML)

Field	Details
Course Name	(Steganography & Watermarking Techniques
Course Code	CY-503
Semester	5
Course Category	Professional Elective Courses
Credits	3
Hours per Week	3L:0T:0P

1. Prerequisites

• Fundamental programming skills (e.g., Python or C)

• Basic knowledge of digital signal processing and multimedia formats (image, audio, video)

• Introductory concepts in computer security and cryptography (hash functions, MACs, basic threat models)

2. Course Learning Objectives

• Equip students with a comprehensive understanding of information hiding concepts, including steganography and digital watermarking, and their historical and contemporary relevance to security and privacy.

• Enable students to design, implement, and evaluate a variety of steganographic and watermarking techniques across multiple media types (text, image, audio, video) using both spatial- and frequency-domain methods.

• Develop students' ability to critically assess the robustness, imperceptibility, and capacity of information-hiding schemes, and to apply appropriate counter-measure and authentication strategies against common attacks.

• Foster proficiency in leveraging modern tools and emerging technologies--such as AI-driven watermark generation and machine-learning based steganalysis--to create adaptive, secure embedding protocols and to detect covert communications.

• Cultivate an awareness of the ethical, legal, and industry standards governing information hiding, preparing students to responsibly apply these techniques in professional and research contexts.

3. Teaching Methodology

• Lectures and Presentations

• Interactive Discussions and Case Studies

• Lab Sessions

• Guest Lectures

4. Evaluation System

Activities	**Class Test Full marks**	**Assignment Full marks**	**Attendance Full marks**	**Total Marks**
CIA-1	25	10	5	40
CIA-2	25	10	5	40
End Semester Examination (ESE)	–	–	–	60
Total				100

5. Course Modules

Module	Topics	Hours
1	Foundations of Information Hiding - Introduction to Information Hiding and its role in security - Historical evolution and real-world use cases - Steganography vs. Encryption: complementary goals - Overview of Digital Watermarking concepts - Threat landscape and ethical/legal considerations - Media carriers and basic multimedia fundamentals * Image formats: BMP, JPEG, PNG - basics of the Human Visual System * Audio formats: WAV, MP3 - perceptual masking principles * Video basics: frame structure, simple compression concepts	5
2	Basic Steganography Techniques - Text steganography: whitespace, synonym substitution, format tricks - Image steganography (spatial domain) * LSB embedding in raw BMP images * Simple palette manipulation for GIFs (basic colour-depth reduction) * Introductory JPEG hiding using DCT coefficient modification - Audio steganography (temporal domain) * Low-bit encoding, echo hiding, silence-interval hiding - Video steganography basics * Frame-level substitution and simple motion-vector embedding	6
3	Fundamentals of Digital Watermarking - Watermarking models and system architecture - Types of watermarks: fragile, semi-fragile, robust - Basic message coding and simple error-correction (parity, Hamming) - Design criteria for a good watermark (imperceptibility, capacity, robustness)	7

	- Spatial-domain watermarking: additive, correlation-based, LSB - Frequency-domain watermarking basics: DCT and DWT embedding - Practical lab: embedding and extracting a watermark in images	
4	Practical Advanced Watermarking & Embedding Protocols - Spread-spectrum watermarking (concept and simple implementation) - Adaptive and hierarchical embedding strategies - Buyer-seller watermarking protocols (overview of privacy-preserving schemes) - Watermarking with side information (basic principles) - Introduction to AI-driven watermark generation (using GANs) - Hands-on project: designing an adaptive watermark for a multimedia stream	8
5	Security, Authentication & Counter-Measures - Core security requirements and basic cryptographic primitives (hashes, MACs) - Watermark security fundamentals - Content authentication techniques (exact, selective, localization) - Common attack vectors * Image-processing attacks: filtering, recompression, JPEG/JPEG-2000 * Geometric attacks: scaling, rotation, cropping, warping * Protocol and cryptographic attacks - Robustness strategies: redundancy, hierarchical embedding - AI-assisted attack detection (overview of deep-learning classifiers) - Lab: evaluating watermark robustness against typical attacks	8
6	Steganalysis, Evaluation & Contemporary Issues - Principles of steganalysis and detection pipelines - Statistical steganalysis basics (higher-order statistics, histogram features) - Machine-learning based steganalysis: SVM,	8

	shallow neural networks, introduction to deep learning models - Calibration techniques (re-compression, resampling) and ROC analysis - Quality and perceptual metrics for stego media - Contemporary topics: * AI-generated media and generative steganography * Legal, ethical, and privacy considerations * Industry standards (e.g., ISO/IEC 13888) and open-source toolkits - Capstone project ideas and guidance	

6. References

Textbooks:

1. Frank Y. Shih, Digital Watermarking and Steganography Fundamentals and Techniques, 2020, 2 nd st Ed. CRC Press, United States. (ISBN No. : 9780367656430)

2. J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications, 2010, 1 Ed. Cambridge: Cambridge University Press, United Kingdom. (ISBN No.: 978 0-52-119019-0)

Reference Books:

1. I. J. Cox, M. L. Miller, J. A. Bloom, T. Kalker, and J. Fridrich, Digital Watermarking and Steganography, 2008, 2 nd Ed. Amsterdam: Morgan Kaufmann Publishers In, United States. (ISBN No. : 978-0-12-372585-1)

2. P. Wayner, Disappearing Cryptography: Information hiding: Steganography and Watermarking, 2008, 3rd ed. Amsterdam: Morgan Kaufmann Publishers In, United States. (ISBN No. : 978-0-08-092270-6)

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
CY-503.1	Recall and list the fundamental concepts of information hiding, including steganography, digital	List	Remember

	watermarking, media carriers, and the basic principles of human visual and auditory perception.		
CY-503.2	Explain the historical evolution, ethical/legal considerations, and the distinction between steganography and encryption, and describe basic spatial- and frequency-domain techniques for images, audio, and video.	Explain	Understand
CY-503.3	Implement elementary steganographic and watermarking algorithms (e.g., LSB embedding, palette manipulation, DCT coefficient modification, additive spatial watermark) to embed and extract hidden data in BMP, JPEG, WAV, and MP4 files using a programming environment provided in the lab.	Implement	Apply
CY-503.4	Analyze the robustness of the implemented watermarks against common attacks (filtering, recompression, scaling, rotation, cropping) by measuring imperceptibility, capacity, detection accuracy, and ROC-curve performance.	Analyze	Analyze
CY-503.5	Evaluate existing watermarking protocols and propose AI/ML-enhanced improvements (e.g., GAN-generated watermarks, ML-based attack detection) that increase security, robustness, and privacy while complying with industry standards such as ISO/IEC 13888.	Evaluate	Evaluate
CY-503.6	Create a complete steganography system that integrates AI-driven watermark generation, machine-learning based steganalysis, and secure authentication mechanisms, and deliver a documented prototype with a performance analysis report meeting the defined	Create	Create

	quality and robustness criteria.		

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	2	1	1	1	-	1	-	-	-	1	-	1
CO2	3	2	2	2	2	3	1	3	-	2	-	2
CO3	3	2	3	2	3	1	-	1	1	1	1	2
CO4	2	3	2	3	2	1	-	1	1	2	1	2
CO5	3	3	3	3	3	2	1	2	1	2	2	3
CO6	3	3	3	3	3	3	2	3	3	3	3	3

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	1	1	1
CO2	2	1	2
CO3	2	3	1
CO4	2	2	1
CO5	3	3	2
CO6	3	3	2

Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(CS)

Field	Details
Course Name	Data Analytics for Fraud Detection
Course Code	CY-504
Semester	5
Course Category	Professional Elective Courses
Credits	3
Hours per Week	3L:0T:0P

1. Prerequisites

• Proficiency in Python or R for data analysis and scripting

• Fundamental statistics and probability (descriptive stats, hypothesis testing, Z-score)

• Basic understanding of relational databases and SQL for data extraction

2. Course Learning Objectives

• This course introduces students to fundamental concepts and applications of the subject

• Students will learn theoretical foundations and practical skills relevant to the field

3. Teaching Methodology

• Lectures and Presentations

• Interactive Discussions and Case Studies

• Lab Sessions

• Guest Lectures

4. Evaluation System

Activities	Class Test Full marks	Assignment Full marks	Attendance Full marks	Total Marks
CIA-1	25	10	5	40
CIA-2	25	10	5	40
End Semester Examination (ESE)	–	–	–	60
Total				100

5. Course Modules

Module	Topics	Hours
1	**Foundations of Fraud & Data Analytics** - Fraud landscape: definition, internal vs. external, common types (financial, insurance, healthcare, e-commerce, identity theft, cyber fraud)\n- Fraud actors, motivations and the fraud-lifecycle framework\n- Core fraud-risk frameworks (ACFE, Basel II) and the role of analytics - proactive vs. reactive\n- Data foundations: transactional, customer-profile, behavioral, device, geolocation, temporal, text\n- Data sources: system logs, bank feeds, claim databases, social/graph data, IoT devices (POS, ATM)\n- Data-quality challenges: missing values, imbalance, noise, skewed distributions\n- Basic data-pre-processing: cleaning, normalization/standardization, categorical encoding\n- Intro to class-imbalance handling (overview of SMOTE/ADASYN)\n- Core statistical concepts for fraud analytics - descriptive stats, Z-score, probability basics, simple hypothesis testing\n- Overview of analytics tool-set: Microsoft Excel, Access, introductory R (scripts, data frames, basic visualisation)	6

2	**Exploratory Data Analysis & Feature Engineering** - EDA techniques: distribution analysis, outlier detection, segmentation, correlation studies\n- Visualisation toolbox: heat-maps, box-plots, time-series charts, network/graph plots, behavioral pattern graphs\n- Feature-engineering fundamentals for fraud detection\n * Transaction velocity & time-window features\n * Risk-scoring and geographic distance calculations\n * Basic behavioural biometrics (typing rhythm, mouse movement)\n * Sequence-pattern extraction (event ordering)\n * Intro to network/graph-based features - link analysis, centrality, community metrics\n- Advanced feature construction: temporal aggregations, rolling statistics, simple text features (TF-IDF, word-counts)\n- Strategies for imbalanced data - oversampling & synthetic data generation overview\n- Practical lab (Python/R) - hands-on EDA, visualisation, and end-to-end feature-creation workflow	7
3	**Rule-Based & Classical Machine-Learning Fraud Detection** - Rule-based detection: business rules, expert systems, decision tables, limitations and hybrid rule + ML approaches\n- Classical supervised models - logistic regression, decision trees, random forest, gradient-boosting basics (XGBoost/LightGBM)\n- Handling class imbalance in supervised learning - cost-sensitive learning, threshold tuning\n- Model evaluation for binary fraud problems\n * Confusion matrix, precision, recall, F1-score\n * ROC-AUC, PR-AUC, cost-based metrics\n * Impact analysis of false positives vs. false negatives\n- Model validation techniques - hold-out split, k-fold cross-validation, simple hyper-parameter tuning\n- Hands-on project: build a baseline rule engine, train a supervised model, compare performance and discuss trade-offs	8
4	**Unsupervised, Semi-Supervised Techniques & Explainability** - Unsupervised anomaly detection methods\n * Clustering (K-Means, DBSCAN)\n * Isolation Forest, One-Class SVM, PCA-based reconstruction scoring\n- Semi-supervised & positive-unlabeled (PU) learning basics for fraud\n- Hybrid approaches - combining rule-based / supervised scores with unsupervised anomaly signals\n- Model explainability fundamentals - feature importance, SHAP, LIME, simple post-hoc visualisations\n- Fairness & bias basics - detecting and mitigating bias in fraud models\n- Practical lab: apply	8

	an unsupervised detector, integrate with a supervised model, generate explanations for predictions	
5	**Fraud Detection System Architecture & Operationalisation** - System components & design patterns - real-time scoring engines, batch vs. streaming pipelines, micro-services and API integration\n- Big-data & streaming technologies overview - Apache Spark/PySpark, Kafka (or Flink) for low-latency scoring\n- Storage options - relational SQL, NoSQL key-value stores, introductory graph DB concepts (Neo4j)\n- Cloud platforms & managed services - AWS SageMaker & Kinesis, Azure ML Studio & Event Hubs, GCP Vertex AI & Pub/Sub (focus on deployment rather than deep cloud engineering)\n- Model deployment basics - containerisation with Docker, orchestration overview with Kubernetes, versioning\n- Monitoring & drift detection - performance alerts, simple statistical drift checks, scheduled retraining workflow\n- Edge & device-level inference - on-device scoring concepts for ATMs, POS terminals, mobile wallets\n- Lab exercise: package a fraud model as a micro-service, set up a streaming scoring pipeline, implement basic monitoring alerts	7
6	**Domain Applications, Governance & Capstone Project** - Domain-specific case studies\n * Banking & credit-card fraud (CNP, charge-back, real-time scoring)\n * Insurance fraud (auto, healthcare, document forgery with OCR)\n * E-commerce & payment fraud (account takeover, coupon abuse, fake reviews)\n * Telecom fraud (SIM-swap, subscription, call-routing fraud)\n- Legal, ethical & regulatory landscape - GDPR, HIPAA, PCI-DSS, ISO 27001, industry-specific compliance\n- Data-privacy, fairness, bias mitigation and ethical use of customer data in fraud analytics\n- Explainable AI requirements and risk communication to stakeholders\n- Fraud-risk management lifecycle - data governance, model governance, incident response\n- Professional skills - reporting & visualisation for non-technical audiences, risk-based decision making\n- Capstone project overview - end-to-end fraud-detection pipeline (ingestion -> preprocessing -> feature engineering -> modelling -> evaluation -> deployment) with presentation expectations\n- Certification pathways - relevance of Google Data Analytics Certificate and other industry-recognised credentials	6

6. References

Textbooks:

1. Data Analytics Using Exel with Accounting and Financial Datasets, 3 Edition: Joseph M. Manzo ISBN: 978-1-4533-3759-2

2. Forensic Analytics: Methods and Techniques for Forensic Accounting Investigations, 2 Edition: Mark J. Nigrini | nd ISBN 9781119585763

3. Fraud and Fraud Detection: A Data Analytics Approach by Sunder Gee, Wiley

Reference Books:

1. Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques: A Guide to Data Science for Fraud Detection, Baesens, Bart, Van Vlasselaer, Veronique, Verbeke, Wouter | ISBN 13: 9781119133124

2. Blokdyk Gerardus, Data analysis techniques for fraud detection, Createspace Independent Publishing Platform

3. Leonard W. Vona, Fraud Data Analytics Methodology: The Fraud Scenario Approach to Uncovering Fraud in Core Business Systems, Wiley

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
CY-504.1	Identify and describe at least five major fraud types, their associated actors, lifecycle stages, and relevant data sources, and explain common data-quality challenges that affect fraud analytics.	Identify	Understand
CY-504.2	Perform exploratory data analysis on a provided fraud dataset, create a minimum of ten engineered features (including temporal, behavioural, and graph-based features), and apply appropriate class-imbalance techniques to prepare the data for modelling.	Perform	Apply
CY-504.3	Build, train, and tune both a rule-based detection engine and at least two supervised machine-learning models (e.g., logistic regression and random forest), evaluate them	Build	Analyze

	using confusion-matrix, precision, recall, F1-score, ROC-AUC, and cost-based metrics, and compare their performance trade-offs.		
CY-504.4	Design and implement an unsupervised or semi-supervised anomaly-detection pipeline, integrate its scores with supervised model outputs, generate feature-level explanations using SHAP or LIME, and assess model fairness by detecting bias against protected attributes.	Design	Evaluate
CY-504.5	Architect, containerize (Docker) and deploy a real-time fraud-scoring micro-service on a streaming platform (Kafka or Spark Structured Streaming) within a cloud environment, and configure monitoring alerts for model drift and performance degradation.	Architect	Create
CY-504.6	Synthesize domain-specific fraud scenarios, regulatory and ethical guidelines, and governance best practices to deliver a complete end-to-end fraud-detection solution, and present a professional report and demonstration to a non-technical audience that meets certification standards.	Synthesize	Create

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	1	2	1	1	-	1	-	1	-	2
CO2	2	3	2	3	3	1	-	1	2	1	1	2
CO3	2	2	3	2	3	1	-	1	2	2	2	2
CO4	2	2	3	3	3	2	-	2	2	1	2	2
CO5	2	1	3	1	3	1	1	1	2	1	3	2
CO6	2	2	2	2	2	3	1	3	2	3	2	2

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	3	2	1
CO2	2	3	1
CO3	2	3	1
CO4	2	3	3
CO5	2	3	1
CO6	2	3	3

Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(CS)

Field	Details
Course Name	Web Application Security
Course Code	CY-505
Semester	5
Course Category	Open Elective Courses
Credits	3
Hours per Week	3L:0T:4P

1. Prerequisites

• Fundamentals of computer networking and TCP/IP (including HTTP/HTTPS basics)

• Experience with a server-side programming language and web development concepts (e.g., Java, Python, PHP, JavaScript, HTML/CSS)

• Basic understanding of operating system concepts, command-line usage, and common security principles (e.g., confidentiality, integrity, availability)

2. Course Learning Objectives

• This course introduces students to fundamental concepts and applications of the subject

• Students will learn theoretical foundations and practical skills relevant to the field

3. Teaching Methodology

• Lectures and Presentations

• Interactive Discussions and Case Studies

• Lab Sessions

• Guest Lectures

4. Evaluation System

Activities	Class Test Full marks	Assignment Full marks	Attendance Full marks	Total Marks
CIA-1	25	10	5	40
CIA-2	25	10	5	40
End Semester Examination (ESE)	_	_	_	60
Total				100

5. Course Modules

Module	Topics	Hours
1	**Foundations of Web and Network Security** - Web Application Basics * Introduction & Architecture * HTTP protocol fundamentals * Common encoding schemes (URL, Base64, HTML) * Enumerating content & functionality - OWASP Top 10 Overview & Core Security Standards (NIST, ISO 27001) - Network & Service Enumeration * Network scanning (port, service discovery) * Directory browsing & brute-forcing * CMS vulnerability scanning basics - Security Misconfigurations & Initial Hardening * Secure defaults, unnecessary service removal - Fundamentals of Input & Output Validation * Whitelisting vs. blacklisting * Basic sanitisation & encoding techniques - Introductory Threat Modeling (STRIDE) and Risk	5

	Assessment	
2	**Authentication, Session Management & Access Controls** - Authentication Principles & Secure Design * Design flaws vs. implementation flaws * Multi-factor authentication basics - Password Policies & Secure Storage * Complexity, lockout, salted hashing (avoid plain MD5) * Password-policy enforcement tools - Session Management * Session fixation, token generation, logout, timeout, Session-ID requirements - CSRF Protection * CSRF tokens, GET vs. POST, Referrer validation - Insecure Direct Object Reference (IDOR) Prevention - Broken Access Control Fundamentals * Least privilege, RBAC, ABAC concepts - Single Sign-On, PKI & Kerberos Basics * SSO overview, certificate handling, Kerberos ticket flow - Intro to OAuth 2.0 / OpenID Connect for modern web apps	6
3	**Injection Attacks & Advanced Input Validation** - Injection Attack Landscape * Interpreted-context injection vectors - SQL Injection (Classic & Advanced) * Error-based, blind, union, parameterised queries - NoSQL, XPath, LDAP, XML & HTTP/Mail Service Injection - Command Injection & Remote Code Execution - File Inclusion & Manipulation * Local File Inclusion (LFI), Remote File Inclusion (RFI) * Arbitrary file download / upload - Cross-Site Scripting (XSS) * Reflected, stored, DOM-based, real-world exploitation - Server-Side Request Forgery (SSRF) - Advanced CSRF Techniques - Comprehensive Input Validation & Output Encoding Strategies * Whitelisting, escaping, URL-encoding, HTML-encoding, content-type checks	8
4	**Secure Development Practices & Source-Code Analysis**	7

	- Secure Coding Practices (OWASP ASVS) * Centralised DB connection, admin-module protection, CAPTCHA, session handling - Coding Standards & Guidelines * Language-specific best practices (Java, ASP.NET, PHP, Perl) - Threat Modeling within the SDLC - Source-Code Vulnerability Analysis * Manual review patterns, automated signatures - Static & Dynamic Application Security Testing (SAST/DAST) * Tool selection, integration into CI/CD - Secure Configuration Management * Cache-control, security headers, SSL/TLS hardening, weak-cipher mitigation - Logging, Auditing & Log-Poisoning Mitigation - Defensive Controls * Clickjacking protection, CSP, HSTS, Cookie security (HttpOnly, Secure flags) - DevSecOps fundamentals - embedding security in CI/CD pipelines	
5	**Database Security & Data Protection** - Database Security Foundations * Data-security requirements, compliance (GDPR, PCI-DSS), risk management - Database Access Control * Authentication, password protection, roles & privileges, system/object privileges - Encryption & PKI for Data at Rest & in Transit * SSL/TLS configuration, certificate basics, key management, AES/RSA usage (conceptual) - Secure Database Links & Auditing * Encrypted link passwords, audit trails, view-based restrictions - Patch Management, Default Settings & Hardening - Monitoring & Incident Logging * Immutable logs, retention, backup strategies - Cloud & NoSQL Database Security Basics * Data masking, tokenization, secure outsourcing considerations	8
6	**Advanced Web Application Penetration Testing & Defensive Strategies** - Advanced Web Application Pen-Testing Methodology (PTES / OWASP) - Advanced SQL Injection exploitation techniques - Advanced XSS (DOM-based bypasses, polyglot payloads) - Authentication Bypass & Privilege Escalation tactics	8

	- File Tampering, Log Poisoning, Cookie Modification attacks - Weak SSL/TLS Cipher exploitation & mitigation - Session Fixation attacks & defenses - Clickjacking & HTTP Header Modification attacks (CSP, HSTS, Referrer-Policy) - Denial-of-Service (DoS) mitigation strategies - Post-exploitation: lateral movement, persistence, privilege escalation - Reporting, Remediation & Auditing Process * CERT-IN audit workflow, NIC staging, deployment best practices - Alignment with industry frameworks (CIS Controls, NIST CSF)	

6. References

Textbooks:

1. "The Web Application Hacker's Handbook", Dafydd Stuttard, Wiley India Pvt. Ltd.

2. " Database Security" , S.Castano, M. Fugini, G. Martella,P. Samarati, Addision-Wesley

Reference Books:

1. " Database Security " Alfred Basta, Melissa Zgola, Cengage Publication, 2012

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
CY-505.1	Identify and describe the core components of web applications, HTTP protocol fundamentals, common encoding schemes, the OWASP Top 10 vulnerabilities, and basic network and service enumeration techniques.	Identify	Remember
CY-505.2	Explain the principles of authentication, session management, CSRF protection, and access-control models (RBAC, ABAC), and illustrate how SSO, PKI, Kerberos, and OAuth 2.0/OpenID Connect operate in modern web environments.	Explain	Understand

CY-505.3	Implement secure input-validation, output-encoding, and parameterized-query techniques to prevent SQL/NoSQL injection, XSS, SSRF, and command-injection attacks in a sample web application.	Implement	Apply
CY-505.4	Analyze source-code and application configurations using static and dynamic analysis tools, perform threat modeling within the SDLC, and formulate remediation recommendations aligned with OWASP ASVS.	Analyze	Analyze
CY-505.5	Evaluate database security controls--including authentication, role-based privileges, encryption at rest and in transit, auditing, and compliance (GDPR, PCI-DSS)--and design a hardened database architecture for a given scenario.	Evaluate	Evaluate
CY-505.6	Design and execute an advanced web-application penetration test following PTES/OWASP methodology, produce a comprehensive remediation report, and integrate automated security testing into a CI/CD pipeline consistent with NIST CSF and CIS Controls.	Design	Create

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	1	1	1	2	1	1	1	1	1	2
CO2	3	3	2	2	1	2	1	2	1	2	1	3
CO3	2	2	3	2	3	2	1	2	1	2	1	2
CO4	2	3	2	3	3	2	1	2	1	3	2	3
CO5	2	2	3	2	3	3	2	2	1	2	2	3
CO6	2	2	3	3	3	3	2	2	2	3	3	3

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	3	2	1
CO2	3	2	2

CO3	2	3	1
CO4	2	3	2
CO5	3	2	3
CO6	2	3	2

Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(AIML)

Field	Details
Course Name	/Operational Technology Security
Course Code	CY-506
Semester	5
Course Category	Open Elective Courses
Credits	3
Hours per Week	3L:0T:0P

1. Prerequisites

• Fundamental understanding of networking concepts and protocols (TCP/IP, OSI model, VLANs, firewalls)

• Basic knowledge of cybersecurity principles and risk management (confidentiality, integrity, availability, threat modeling, incident response)

• Introductory exposure to industrial control systems or operational technology (PLC, SCADA, DCS) and related engineering concepts

2. Course Learning Objectives

• This course introduces students to fundamental concepts and applications of the subject

• Students will learn theoretical foundations and practical skills relevant to the field

3. Teaching Methodology

• Lectures and Presentations

• Interactive Discussions and Case Studies

• Lab Sessions

• Guest Lectures

4. Evaluation System

Activities	Class Test Full marks	Assignment Full marks	Attendance Full marks	Total Marks
CIA-1	25	10	5	40
CIA-2	25	10	5	40
End Semester Examination (ESE)	–	–	–	60
Total				100

5. Course Modules

Module	Topics	Hours
1	**Foundations of Operational Technology and Industrial Control Systems** - Executive summary, purpose, audience and document structure - OT evolution and why it differs from IT - Core OT components: PLC, RTU, DCS, SCADA, building-automation, physical-access and safety systems - Safety, reliability and availability fundamentals for OT - Typical industrial sectors and OT environments - Purdue Reference Model (Levels 0-5) and common network topologies - Key OT protocols (Modbus, DNP3, IEC 60870-5-104, OPC-UA, Profinet, EtherNet/IP) and their inherent security weaknesses - Introduction to data sources for AI-enabled	8

	monitoring in OT	
2	**Threat Landscape and Risk Management for OT** - Threat actors and vectors specific to OT (nation-state, insiders, cyber-criminals) - Landmark case studies: Stuxnet, Triton, Ukraine power-grid attacks - Core risk concepts and terminology for OT - OT risk-assessment process: Identify, Analyze, Prioritize - Mitigation strategies and controls aligned with risk levels - Continuous risk monitoring, metrics and dashboards - Special risk areas: supply-chain, safety-critical systems, geographically distributed assets - Applying the NIST RMF (Prepare -> Monitor) to OT environments - Using lightweight AI/ML scoring to prioritize high-impact risks	7
3	**OT Security Frameworks, Standards and Governance** - Key standards & guidance: NIST SP 800-82, ISA/IEC 62443 series, IEC 60870-5-104, IEC 61508/61511 - International consortia and industry groups (CIPAC, I3P, IEC TC 57/65, IEEE, ISA, ISASecure) - NIST Cybersecurity Framework functions for OT (Identify, Protect, Detect, Respond, Recover) with OT-specific sub-categories - Mapping ISA/IEC 62443 security levels to the NIST CSF - Governance structures: policy, roles, responsibilities, and compliance reporting - Emerging AI governance considerations for OT (model validation, bias, explainability) - Regulatory landscape overview (e.g., NERC CIP, EU NIS-2, national critical-infrastructure laws)	6
4	**OT Security Architecture and Defense-in-Depth** - Developing an OT cybersecurity strategy: defense-in-depth, risk-based, resilience-focused - Layered security architecture: * Layer 1 - Security Management (policy, governance, risk) * Layer 2 - Physical Security (perimeter, environmental controls) * Layer 3 - Network Security (segmentation, zoning, industrial DMZ, firewalls)	8

	* Layer 4 - Hardware Security (trusted boot, firmware integrity) * Layer 5 - Software Security (application hardening, secure code) - Architecture models for DCS, PLC, SCADA and IIoT-enabled OT - Secure remote-access design (jump hosts, VPN, MFA, least-privilege) - Field I/O (Purdue Level 0) protection techniques - IIoT and edge-device security considerations - Impact of security controls on safety, availability and reliability - Leveraging AI-driven analytics for network-traffic baselining and anomaly detection	
5	**OT Security Operations: Hardening, Monitoring & Incident Response** - Hardening guidelines for PLCs, RTUs, DCS, SCADA servers and IIoT devices - Patch-management and flaw-remediation processes tailored to OT constraints - Time-synchronization best practices (NTP/PTP) for reliable logging - OT logging, telemetry collection and challenges of continuous monitoring - IDS/IPS for OT: signature-based vs. anomaly-based, optimal deployment points - Building and maintaining a Maintenance Tracking Capability - OT-specific incident-response lifecycle (preparation -> post-incident analysis) - Recovery & restoration planning (safe-state procedures, business-continuity integration) - AI-enabled automated detection and response playbooks (e.g., model-driven containment)	5
6	**Building and Governing an OT Cybersecurity Program** - Chartering the OT cybersecurity program and scoping its mandate - Business case development: ROI, stakeholder alignment and executive briefing - Governance structures and cross-functional teams (operations, IT, safety, compliance) - Defining OT-specific policies, procedures and standards - Designing and delivering OT cybersecurity awareness and training (including AI-tool usage) - Implementing the OT Risk Management Framework (RMF) within the program - Continuous-improvement cycle: metrics, audits,	8

	lessons learned - Emerging topics: IIoT security, cloud-based OT monitoring, supply-chain risk mitigation, AI/ML for predictive security, upcoming regulatory trends	

6. References

Textbooks:

1. Massimo Nardone, 1st Edition, Apress -- Industrial Control System (ICS) and Operational Technology (OT) Security: An Introduction to Securing a Complex Industrial Environment"

2. "Tyson Macaulay & Bryan L. Singer, 1st Edition, Auerbach Publications -- Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS"

Reference Books:

1. "(Editors) -- Cyber-security of SCADA and Other Industrial Control Systems, 1st Edition, Springer International Publishing"

2. "Pascal Ackerman, 1st/2nd Edition, (Publisher: depends on edition) -- Industrial Cybersecurity: Efficiently Secure Critical Infrastructure Systems"

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
CY-506.1	Identify and list at least five core Operational Technology components (e.g., PLC, RTU, DCS, SCADA, building-automation) and three key OT communication protocols, and describe the primary security weaknesses associated with each protocol.	Identify	Remember
CY-506.2	Explain the major OT threat actors, vectors, and landmark case studies (such as Stuxnet, Triton, and the Ukraine power-grid attack) and summarize how the NIST RMF and ISA/IEC 62443 frameworks address these threats.	Explain	Understand
CY-506.3	Apply the layered-defense-in-depth model to design a secure OT	Apply	Apply

	architecture for a given industrial scenario, selecting appropriate controls from NIST 800-82, ISA/IEC 62443, and incorporating AI-enabled traffic-baselining for the network-security layer.		
CY-506.4	Analyze real-time OT network telemetry using an AI/ML anomaly-detection model to identify suspicious traffic patterns, and produce a risk-prioritization report that ranks findings according to potential safety and availability impact.	Analyze	Analyze
CY-506.5	Evaluate a set of mitigation strategies and incident-response playbooks by measuring their effectiveness with AI-driven scoring metrics, and recommend improvements that achieve at least a 20 % reduction in mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR).	Evaluate	Evaluate
CY-506.6	Design and document a comprehensive OT cybersecurity program that integrates governance, policy, continuous-risk monitoring, AI/ML governance, and compliance with NERC CIP, EU NIS-2, and IEC 62443, and present an implementation roadmap with measurable milestones for the next 12 months.	Design	Create

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	2	1	-	-	-	-	-	-	-	1	-	-
CO2	3	2	2	3	-	2	-	1	-	3	-	2
CO3	3	2	3	2	3	2	-	2	2	2	2	2
CO4	3	3	2	3	3	2	-	1	2	3	2	2
CO5	2	3	3	3	3	2	-	1	2	3	3	2
CO6	3	3	3	2	3	3	2	3	3	3	3	3

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	-	-	-
CO2	-	-	1
CO3	3	3	1
CO4	3	3	1
CO5	3	3	1
CO6	3	2	3

Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(Cyber Security)

Field	Details
Course Name	Database Management Systems
Course Code	CY-507
Semester	5
Course Category	Program Core Courses
Credits	3
Hours per Week	3L:0T:4P

1. Prerequisites

• Basic knowledge of Database Management Systems

• Programming fundamentals

2. Course Learning Objectives

• To provide a comprehensive understanding of the fundamental principles, architecture, and purpose of modern database management systems.

• To equip students with the theoretical knowledge and practical skills to design well-structured and normalized relational database schemas using conceptual and logical modeling techniques.

• To develop proficiency in using the Structured Query Language (SQL) for data definition, manipulation, and complex querying, grounded in the theoretical foundations of relational algebra.

• To introduce the core principles of transaction processing, concurrency control, and recovery, emphasizing their role in maintaining data integrity and consistency in multi-user environments.

• To foster an appreciation for the underlying mechanisms of database implementation, including data storage, indexing, and query optimization, and to introduce fundamental concepts of database security.

3. Teaching Methodology

• Lectures and Presentations

• Interactive Discussions and Case Studies

• Lab Sessions

• Guest Lectures

4. Evaluation System

Activities	Class Test Full marks	Assignment Full marks	Attendance Full marks	Total Marks
CIA-1	25	10	05	40
CIA-2	25	10	05	40
End Semester Examination (ESE)	-	-	-	60
			Total	100 marks

5. Course Modules

Module	Topics	Hours
1	**Foundations of Modern Database Systems** Core Concepts: Purpose and applications of database systems, comparison with file systems, characteristics of the database approach. Database Architecture: The three-schema architecture (internal, conceptual, external), data independence, overall system structure. The Data Modeling Landscape: Introduction to different data models (Relational, NoSQL), and use cases (OLTP vs. OLAP). Database Users and Administrators: Roles and responsibilities in a database environment. Introduction to the Relational Model: Core concepts of relations, attributes, domains, and schemas. Introduction to Transactions: A high-level overview of transactions, their purpose, and the need for concurrency and recovery.	6
2	**Conceptual and Logical Database Design** Entity-Relationship (ER) Model: Entities, attributes (simple, composite, multi-valued), and entity sets.	7

	Relationships and Constraints: Relationship sets, degree, cardinality constraints, and participation constraints. Advanced ER Design: Weak entity sets, enhanced ER (EER) concepts like specialization and generalization (overview). The Relational Model In-Depth: Keys (Super, Candidate, Primary, Foreign) and integrity constraints (Entity, Referential). Mapping ER to Relational Schema: A systematic process for converting ER and EER diagrams into a set of relational tables.	
3	**Relational Algebra and SQL** Relational Algebra: The theoretical foundation for SQL. Operations: Select, Project, Union, Set Difference, Cartesian Product, Rename, and Joins. SQL Data Definition (DDL): CREATE, ALTER, DROP statements for tables, defining constraints (PRIMARY KEY, FOREIGN KEY, NOT NULL, UNIQUE, CHECK). SQL Data Manipulation (DML): SELECT, INSERT, UPDATE, DELETE statements. Complex Queries in SQL: Aggregate functions, GROUP BY and HAVING clauses, nested queries, and various JOIN operations (INNER, LEFT/RIGHT OUTER). Views: Creating virtual tables with CREATE VIEW, understanding their use for security and simplicity. SQL Injection: Introduction to the vulnerability and best practices for prevention (e.g., parameterized queries).	8
4	**Relational Database Design Theory and Normalization** Informal Design Guidelines: Semantics of attributes, reducing redundant information, and minimizing null values. Functional Dependencies (FDs): Definition, inference rules (Armstrong's Axioms), and finding minimal covers. The Normalization Process: Progression from First (1NF), Second (2NF), and Third (3NF) Normal Forms. Boyce-Codd Normal Form (BCNF): A stronger definition of 3NF and its comparison. Properties of Decompositions: Lossless-join and dependency-preservation properties of decompositions. Higher Normal Forms (Overview): A conceptual introduction to the problems solved by 4NF (Multi-valued Dependencies) and 5NF (Join Dependencies).	7
5	**Transaction Processing and Concurrency Control** Transaction Concepts: Transaction states, ACID	7

	properties (Atomicity, Consistency, Isolation, Durability) explained in detail. Concurrency and Schedules: The problem of concurrent execution, serializability (conflict and view), and recoverability. Concurrency Control Strategies: Pessimistic Approach: Lock-based protocols, Two-Phase Locking (2PL). Optimistic Approach: Validation-based protocols. Deadlock Handling: Deadlock prevention, detection, and recovery strategies. Database Recovery Techniques: Concepts of log-based recovery, deferred vs. immediate updates, and checkpoints.	
6	**Storage, Indexing, and Database Security** Storage and File Structures: Overview of physical storage media, record organization, and file organization techniques. Indexing Structures: Ordered indices, primary vs. secondary indices, and an introduction to B+ Tree indexes. Query Processing and Optimization: Overview of query processing steps, measures of query cost, and the role of the query optimizer. Database Security and Administration: Access Control: Discretionary Access Control using GRANT and REVOKE commands. User and Role Management: Creating and managing database users and roles for privilege separation. Data Protection: Introduction to database auditing and the importance of encryption (at rest and in transit).	7

6. References

Textbooks:

1. Database System Concepts by Abraham Silberschatz, Henry Korth, and S. Sudarshan

2. Data base Management Systems, Raghurama Krishnan, Johannes Gehrke, TATA McGrawHill 3rd Edition.

Reference Books:

1. Fundamentals of Database Systems, Elmasri Navathe Pearson Education.

2. An Introduction to Database systems, C.J. Date, A.Kannan, S.Swami Nadhan, Pearson, Eight Edition for UNIT III.

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
CY-507.1	Explain the fundamental concepts of database systems, including their architecture, the distinction between relational and NoSQL models for different use cases like OLTP and OLAP, and the purpose of transactions.	Explain	Understand
CY-507.2	Design logical database schemas using Entity-Relationship (ER) modeling techniques and translate these conceptual models into a relational schema with appropriate keys and integrity constraints.	Design	Apply
CY-507.3	Formulate complex SQL queries to define, manipulate, and retrieve data, utilizing joins, aggregate functions, and subqueries to extract meaningful information for applications and data analysis.	Formulate	Apply
CY-507.4	Analyze relational database schemas for design anomalies using the principles of functional dependencies and normalization, and refine them to achieve at least Boyce-Codd Normal Form (BCNF).	Analyze	Analyze
CY-507.5	Analyze transaction processing concepts by explaining the ACID properties, evaluating schedules for serializability, and comparing concurrency control and recovery mechanisms used to ensure data integrity.	Analyze	Analyze
CY-507.6	Implement database security policies using access control mechanisms and explain how storage structures and indexing, such as B+ trees, impact query performance in data-intensive systems.	Implement	Apply

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	1	1	1	-	-	-	-	1	-	2
CO2	3	2	3	1	2	1	-	1	1	2	1	1
CO3	3	3	2	2	3	-	-	-	-	1	-	1
CO4	3	3	3	2	1	-	-	-	-	1	-	1
CO5	3	3	2	2	1	1	-	1	-	1	-	2
CO6	3	2	2	2	3	2	1	2	-	1	-	2

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	3	1	2
CO2	3	1	2
CO3	3	2	2
CO4	3	1	1
CO5	3	1	2
CO6	3	2	3