Curriculum Semester-III

Executive M.Tech in Computer Science and Engineering

(With Specialization in Cloud Computing & Blockchain)

Semesters	Subject Code	Courses Name	Category	L	T	P	Credits
Semester-3	CS3532XCS	Elective-3	DE	3	0	0	**3**
	CS3532XCS	Elective-4	DE	3	0	0	**3**
	CS35351CS	Project work / Dissertation-I	PW	-	-	16	**8**
			Total Credits				**14**

Tentative List of Elective Subjects (may be updated as and when required)

Elective-3	Elective-4
Next Generation Computing (CS35321CS)	Distributed Ledger Technologies and Applications (CS35324CS)
Security & Privacy of AI (CS35322CS)	Cloud Security (CS35325CS)
Cyber Physical System Security (CS35323CS)	Digital Forensics (CS35326CS)

Elective 3-NEXT GENERATION COMPUTING

Subject Code: CS35321CS	Subject Type: DE (Elective-3)	Evaluation Scheme: MSE (30), TA (20), ESE (50)	L-T-P: 3-0-0 (3)

Pre-Requisites: Computer Organization & Architecture, Linear Algebra, Complex Analysis, Probability Theory, Foundations of Machine Learning or Pattern Recognition, Proficiency in a High-Level Programming Language (Python, C/C++)

Course Objective: To analyze GPU architectures and design scalable parallel computing strategies for massive AI workloads. To establish the mathematical foundations of quantum mechanics, quantum algorithms, and Quantum Machine Learning (QML). To investigate neuromorphic computing paradigms, spiking neural networks, and biologically inspired learning.

Course Outcomes: At the end of the course, the student will be able to

CO	Course Outcomes
CO-1	Evaluate GPU architectures, optimize kernel-level execution, and design scalable distributed training pipelines for deep learning models.
CO-2	Analyze quantum states and circuits to implement foundational quantum algorithms and Parameterized Quantum Circuits (PQCs) for ML tasks.
CO-3	Design and simulate Spiking Neural Networks (SNNs) and critically evaluate neuromorphic hardware for energy-efficient cognitive computing.
CO-4	Apply advanced model compression techniques for Edge AI deployment and critically evaluate emerging optical, analog, and in-memory computing paradigms.

Syllabus:

Unit-1: High-Performance Computing and Distributed AI Architectures

Memory hierarchies, computational bottlenecks, and the Roofline performance model. GPU Architecture: Streaming multiprocessors, warp execution, and the SIMT paradigm. CUDA programming fundamentals: Thread hierarchy, memory coalescing, and synchronization mechanisms. Advanced tensor operations and mixed-precision optimization. Distributed Deep Learning: Strategies for data, tensor, and pipeline parallelism; gradient synchronization; and memory optimization frameworks (ZeRO, FSDP) for massive language models.

Unit-2: Quantum Computing Foundations and Machine Learning

Mathematical foundations: Qubits, superposition, entanglement, and Dirac notation. Universal quantum gate sets and circuit design. Foundational algorithms: Quantum Fourier Transform (QFT), Quantum Phase Estimation (QPE), and Grover's search algorithm. Quantum Machine Learning (QML): Mapping classical data to quantum states (Amplitude, basis encoding). Parameterized Quantum Circuits (PQCs), expressibility, and gradient computation (parameter shift rule). Optimization challenges in the NISQ era: Barren plateaus and error mitigation.

Unit-3: Neuromorphic Computing and Bio-Inspired Systems

Biological plausibility in computation: Membrane potential dynamics and Leaky Integrate-and Fire (LIF) neuron models. Neural coding schemes: Rate, temporal, and population coding. Synaptic plasticity and bio-inspired learning: Hebbian learning and Spike-Timing Dependent Plasticity (STDP). Training SNNs: Surrogate gradient methods and backpropagation through time (BPTT). Architectural overview and energy efficiency analysis of contemporary neuromorphic hardware accelerators.

Unit-4: Edge AI, Model Compression and Post-CMOS Paradigms

The Edge-Fog-Cloud continuum and latency-constrained AI deployment. Model compression techniques: Post-training quantization, quantization-aware training, unstructured/structured pruning, and knowledge distillation. Federated learning paradigms and communication efficiency. Survey of emerging post-CMOS architectures: Analog in-memory computing (crossbar arrays), photonic/optical neural networks, DNA computing concepts, and the theoretical thermodynamic limits of computational energy efficiency.

Learning Resources:

Text Books:

1. Programming Massively Parallel Processors, Kirk D.B., Hwu W.W. Morgan Kaufmann 2022 (4th Ed.).
2. TinyML: Machine Learning with TensorFlow Lite, Warden P., Situnayake D. O'Reilly Media 2020.
3. Deep Learning, Goodfellow I., Bengio Y., Courville A. MIT Press 2016.
4. Quantum Computation and Quantum Information, Nielsen M.A., Chuang I.L. Cambridge Univ. Press 2010 (10th Ed.)

Reference Books:

1. Computer Architecture: A Quantitative Approach, Hennessy J., Patterson D.
2. Introduction to Quantum Computing, Rieffel E., Polak W. MIT Press.
3. Spiking Neuron Models, Gerstner W., Kistler W.M. Cambridge Univ. Press.

SECURITY & PRIVACY OF AI

Subject Code: CS35322CS	**Subject Type:** DE (Elective-3)	**Evaluation Scheme:** MSE (30), TA (20), ESE (50)	**L-T-P:** 3-0-0 (3)

Pre-Requisites: Machine Learning basics, Deep Learning fundamentals, Cryptography and Network Security (basic), Probability & Statistics

Course Objective: To understand security threats and privacy risks in AI/ML systems. To study adversarial machine learning attacks and defenses. To explore privacy-preserving AI techniques. To design secure and trustworthy AI systems.

Course Outcomes: At the end of the course, the student will be able to

CO	Course Outcomes
CO1	Understand security and privacy fundamentals in AI systems
CO2	Analyze adversarial attacks and threat models
CO3	Apply defense mechanisms to secure AI models
CO4	Implement privacy-preserving ML techniques
CO5	Design and evaluate secure AI applications

Syllabus:

Unit I: Foundations of AI Security and Privacy: Introduction to AI Security and Privacy: Evolution of AI systems and emerging security concerns, Importance of security and privacy in AI applications, Differences between traditional cybersecurity and AI security, Real-world examples of AI failures and attacks; Threat Models in AI: White-box, Black-box, Grey-box attack models, Attacker capabilities and knowledge assumptions, Training-time vs inference-time attacks, Active vs passive adversaries; Security Goals in AI Systems: Confidentiality, Integrity, Availability (CIA triad), Authenticity and accountability in AI, Model robustness and reliability; Privacy Risks in AI Systems: Data leakage and information exposure, Risks in centralized vs distributed learning, Privacy concerns in datasets and model outputs; Trustworthy AI Principles: Robustness and reliability, Fairness and bias mitigation, Explainability and interpretability, Transparency and accountability; Overview of Adversarial Machine Learning.

Unit II: Adversarial Machine Learning: Evasion Attacks (Test-Time Attacks): Concept of adversarial examples, Gradient-based attacks (FGSM, PGD), Optimization-based attacks, Physical-world adversarial attacks; Poisoning Attacks (Training-Time Attacks): Data poisoning techniques, Label flipping and clean-label attacks, Impact on model performance; Backdoor Attacks: Trigger-based attacks, Trojan attacks in neural networks, Detection challenges; Real-World Adversarial Examples: Adversarial images and patches, Attacks in NLP and speech systems, Attacks in autonomous systems; Attack Models and Scenarios: Active vs passive attacks, Training vs inference attacks, Targeted vs untargeted attacks.

Unit III: Defense Mechanisms in AI: Adversarial Training: Basic concept and formulation, Robust training techniques, Trade-off between accuracy and robustness; Out-of-Distribution (OOD) Detection: Definition and importance, Detection methods, Relationship with adversarial examples; Certified Robustness Methods: Formal robustness guarantees, Randomized smoothing, Verification techniques; Defense Against Poisoning & Backdoor Attack: Data sanitization techniques, Anomaly detection methods, Robust learning algorithms; Secure Model Evaluation: Robustness evaluation metrics, Benchmark datasets and testing strategies, Adversarial testing frameworks; Robust ML System Design: Secure ML pipelines, Model hardening techniques, Deployment considerations.

Unit IV: Privacy-Preserving Machine Learning: Privacy Risks in ML Models: Data exposure during training and inference, Leakage through model outputs, Privacy vs utility trade-off; Membership Inference Attacks (MIA): Attack methodology, Overfitting and privacy leakage, Defense strategies; Model Inversion & Property Inference: Inferring sensitive attributes, Class reconstruction attacks, Risks in healthcare and biometrics; Model Extraction Attacks: Stealing model parameters, Query-based attacks, Surrogate model construction; Differential Privacy (DP): Definition and principles, epsilon privacy parameter, DP in machine learning (DP-SGD); Secure Multi-Party Computation (SMC): Secure collaborative computation, Secret sharing techniques, Applications in ML; Homomorphic Encryption (HE): Computation on encrypted data, Types of HE, Applications in secure AI; Federated Learning Privacy: Distributed training framework, Secure aggregation, Privacy risks and mitigation.

Unit V: Security & Privacy in Modern AI Systems: Security in Deep Learning Models: Security in CNNs (vision systems), Security in LLMs (prompt injection, data leakage), Security in AI agents and autonomous systems; Privacy in AI Applications: Privacy in NLP systems, Privacy in computer vision (face recognition risks), Data anonymization techniques; Secure Deployment of AI Systems: Secure model serving, Monitoring and incident response, AI system lifecycle security; Trusted Execution Environments (TEE): Secure enclaves (Intel SGX, ARM TrustZone), Confidential computing, Secure inference; AI Governance, Ethics, and Regulations: GDPR and data protection laws, Ethical AI principles, Responsible AI frameworks; Case Studies and Applications: Healthcare AI (privacy-sensitive data), Financial fraud detection systems, Recommendation systems, Smart cities and IoT security.

Learning Resources:

Text Books:

1. Jason Edwards, Adversarial Machine Learning: Mechanisms, Vulnerabilities, and Strategies for Trustworthy AI, Wiley, 2026.
2. Anthony D. Joseph et al., Adversarial Machine Learning, Cambridge University Press, 2019.

Reference Books:1. Ehsan Nowroozi et al. (Eds.), Adversarial Example Detection and Mitigation Using Machine Learning, Springer, 2025.

CYBER PHYSICAL SYSTEM SECURITY

Subject Code: CS35323CS	**Subject Type:** DE (Elective-3)	**Evaluation Scheme:** MSE (30), TA (20), ESE (50)	**L-T-P:** 3-0-0 (3)

Pre-Requisites: Computer Networks, Operating Systems, Control Systems, Cryptography, Embedded Systems, Programming (C/Python), Basic Knowledge of Distributed Systems

Course Objective: To develop a deep understanding of security challenges, threat models, and defense mechanisms in cyber-physical systems (CPS). To enable students to design resilient, secure, and trustworthy systems that integrate computation, networking, and physical processes.

Course Outcomes: At the end of the course, the student will be able to

CO	Course Outcomes
CO-1	Analyze the architecture, components, and threat landscape of cyber-physical systems
CO-2	Identify vulnerabilities and design secure CPS architectures with formal guarantees
CO-3	Implement security mechanisms for embedded, networked, and control-based systems
CO-4	Evaluate resilience, safety, and trustworthiness of CPS under adversarial conditions

Syllabus:

Unit-1: Foundations of Cyber-Physical Systems

Introduction to CPS: architecture, components (sensors, actuators, controllers, communication networks), Modeling of CPS: hybrid systems, discrete-continuous interactions, Applications: smart grids, autonomous vehicles, industrial control systems (ICS), healthcare systems, Threat landscape: attack surfaces, adversary models, safety vs security interplay, Fundamental principles of CPS security and resilience.

Unit-2: Vulnerabilities and Attack Mechanisms in CPS

Attacks on sensing and actuation: spoofing, false data injection, replay attacks, Network-level attacks: DoS, man-in-the-middle, routing attacks in CPS networks, Control-layer attacks: stealthy attacks on control loops, zero-dynamics attacks, Hardware and embedded vulnerabilities: side-channel attacks, firmware attacks, Case studies: Stuxnet, Ukraine power grid attack, attacks on autonomous systems.

Unit-3: Security Mechanisms for CPS

Secure communication protocols for CPS and IoT systems, Cryptographic techniques: lightweight cryptography, key management in constrained devices, Authentication and access control in CPS environments, Intrusion detection and anomaly detection using machine learning, Secure state estimation and resilient control techniques, Blockchain integration for CPS security and trust management.

Unit-4: Resilience, Safety, and Emerging Trends

Fault tolerance and resilience in CPS under adversarial conditions, Formal methods for CPS security verification (model checking, theorem proving), Safety-critical system design and standards (IEC 62443, NIST CPS framework), Risk assessment and threat modeling methodologies, Privacy in CPS (data protection in smart environments), Emerging areas: digital twins, AI-driven CPS security, edge/IoT security, autonomous systems security.

Learning Resources:

Text Books:

1. Rajeev Alur, Principles of Cyber-Physical Systems, MIT Press.
2. Al-Sakib Khan Pathan, Securing Cyber-Physical Systems, CRC Press.

Reference Books:

1. Kim Zetter, Countdown to Zero Day (Stuxnet).
2. S. Sridhar, A. Hahn, M. Govindarasu, Cyber-Physical System Security for the Smart Grid.
3. Dieter Gollmann, Computer Security, Wiley.
4. Cardenas, Amin, Sastry – Research papers on CPS security.

Elective 4
DISTRIBUTED LEDGER TECHNOLOGIES AND APPLICATIONS

Subject Code: CS35324CS	**Subject Type:** DE (Elective-4)	**Evaluation Scheme:** MSE (30), TA (20), ESE (50)	**L-T-P:** 3-0-0 (3)

Pre-Requisites: NIL

Course Objective: To provide an understanding of Distributed Ledger Technology, blockchain architecture, and consensus mechanisms, and to develop skills for designing smart contracts and decentralized applications while exploring real-world applications and emerging trends.

Course Outcomes: At the end of the course, the student will be able to

CO	Course Outcomes
CO-1	Analyze the principles of Distributed Ledger Technology, cryptographic mechanisms, and blockchain architecture.
CO-2	Evaluate different consensus algorithms and security mechanisms used in blockchain systems.
CO-3	Design and implement smart contracts and decentralized applications using platforms like Ethereum and Hyperledger.
CO-4	Assess real-world applications of blockchain technology and propose suitable solutions for domain-specific problems.

Syllabus:

Unit-1: Foundations of Distributed Ledger Technology

Distributed Systems Fundamentals: Client-server vs Peer-to-Peer systems, Distributed trust and fault tolerance, Introduction to DLT: Centralized vs Distributed vs Decentralized systems, Blockchain as a DLT, Cryptographic Foundations: Hash functions (SHA-256), Digital signatures and public-key cryptography, Merkle Trees, Bitcoin Architecture: Transactions and UTXO model, Block structure and chain formation, Limitations of traditional systems and need for DLT.

Unit-2: Blockchain Architecture and Consensus Mechanisms

Blockchain Architecture: Blocks, nodes, ledgers, Full nodes vs light nodes, Consensus Algorithms: Proof of Work (PoW), Proof of Stake (PoS), Delegated PoS (DpoS), Byzantine Fault Tolerance (PBFT), Mining and Incentive Mechanisms, Forks and Consensus Failures, Security Issues: Double spending, 51% attack, Sybil attack, Permissioned vs Permissionless Blockchain.

Unit-3: Applications, Case Studies and Emerging Trends

Financial Applications: Bitcoin, Ethereum, Decentralized Finance (DeFi), Enterprise Applications: Supply chain management, Healthcare systems, Identity management (Digital ID), Advanced Topics: NFTs (Non-Fungible Tokens), Web3 and decentralized internet, Blockchain interoperability, Integration: Blockchain with IoT and AI, Legal, ethical, and regulatory challenges, Scalability and future directions.

Unit-4: Smart Contracts and Blockchain Platforms

Smart Contracts: Definition, lifecycle, execution model, Ethereum Platform: Accounts, transactions, gas, Ethereum Virtual Machine (EVM), Solidity Programming (basics): Variables, functions, events, Hyperledger Fabric: Permissioned blockchain, Channels and chaincode, Decentralized Applications (Dapps), Tokenization: Cryptocurrencies, ERC standards (ERC-20, ERC-721).

Learning Resources:

Text Books:

1. D. Hellwig, G. Karlic, and A. Huchzermeier, Build Your Own Blockchain: A Practical Guide to Distributed Ledger Technology. Springer, 2020.
2. S. Tanwar, Blockchain Technology: From Theory to Practice. Springer, 2022.

Reference Books:

1. I. Bashir, Mastering Blockchain, 4th ed. Packt Publishing, 2023.
2. R. Pandey, S. Goundar, and S. Fatima, Distributed Computing to Blockchain: Architecture, Technology, and Applications. Academic Press (Elsevier), 2023.
3. P. M. Jeyanthi, Ed., Distributed Ledger Technology in Communication: Integration of IoT, Blockchain and Metadata. Springer, 2026.

CLOUD SECURITY

Subject Code: CS35325CS	**Subject Type:** DE (Elective-4)	**Evaluation Scheme:** MSE (30), TA (20), ESE (50)	**L-T-P:** 3-0-0 (3)

Pre-Requisites: Computer Networks, Cloud Computing, Cryptography & Network Security

Course Objective: To provide an in-depth understanding of security challenges and solutions in cloud computing environments, enabling students to design, analyze, and implement secure cloud architectures while addressing issues related to data protection, privacy, identity management, and compliance in distributed systems.

Course Outcomes: At the end of the course, the student will be able to

CO	Course Outcomes
CO-1	Analyze security threats, vulnerabilities, and risk models specific to cloud computing environments
CO-2	Design secure cloud architectures incorporating identity management, encryption, and access control mechanisms
CO-3	Evaluate cloud security solutions including virtualization security, container security, and network protection techniques
CO-4	Apply security governance, compliance frameworks, and privacy-preserving techniques in real-world cloud deployments

Syllabus:

Unit-1: Introduction to Cloud Security

Cloud computing models (IaaS, PaaS, SaaS) and deployment models (public, private, hybrid), shared responsibility model, cloud threat landscape, attack surfaces in cloud environments, risk assessment and threat modeling, security challenges in multi-tenant environments, data lifecycle in cloud, fundamentals of trust and security requirements.

Unit-2: Identity, Access Control and Data Security

Identity and Access Management (IAM), authentication mechanisms (multi-factor authentication, federated identity), authorization models (RBAC, ABAC), cryptographic techniques for cloud (encryption at rest and in transit), key management systems, secure data storage, data masking, tokenization, and privacy preservation in cloud systems.

Unit-3: Infrastructure and Network Security in Cloud

Virtualization security, hypervisor vulnerabilities, container security and orchestration platforms (Docker, Kubernetes), network security in cloud (VPCs, firewalls, intrusion detection/prevention systems), secure API design, zero-trust architecture, security monitoring and incident response in cloud environments.

Unit-4: Advanced Cloud Security and Governance

Cloud security frameworks (CSA, NIST), compliance standards (ISO 27001, GDPR), security auditing and logging, DevSecOps practices, secure software development in cloud, cloud forensics, privacy-preserving techniques (homomorphic encryption, differential privacy), emerging trends such as confidential computing and secure multi-party computation.

Learning Resources:

Text Books:

1. Ronald L. Krutz & Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Wiley.
2. Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy, O'Reilly.
3. NIST Special Publications on Cloud Security.

DIGITAL FORENSICS

Subject Code: CS35326CS	Subject Type: DE (Elective-4)	Evaluation Scheme: MSE (30), TA (20), ESE (50)	L-T-P: 3-0-0 (3)

Pre-Requisites: Computer Networks, Operating System and Programming

Course Objective: To explore the depths of various digital incident domains, gain practical skills in detecting cyberattacks and incidents using commercial, open-source, and freeware tools, and develop case-oriented procedures for emerging scenarios.

Course Outcomes: At the end of the course, the student will be able to

CO	Course Outcomes
CO-1	Understand the significance of digital evidences and basic digital forensics procedures for conducting the examination on different digital devices.
CO-2	Understand digital forensics and incident response, data acquisition and validation, and demonstrate e-discovery tools.
CO-3	Understand how to extract & examine logs or artifacts from electronic evidences.
CO-4	Understand investigation procedure of volatile and non-volatile memories, operating systems, file systems, and networks.
CO-5	Devise methodologies and techniques for forensic investigation of modern digital devices.

Syllabus:

Unit-1: Introduction to Digital Forensics

Introduction to Digital Forensics, Stages of Forensic: acquisition or imaging, analysis and reporting standards, Chain of custody, Domains of Digital Forensics, Forensic Imaging, IT Act 2000, IT Act Amendments, DPDP Act, Privacy Preserving Forensics, Data De-Duplication, Types of Electronic Evidences and their Artifacts.

Unit-2: Volatile and Non-Volatile Memory Forensics

Volatile and Non-Volatile Memory Forensics, Tools and Techniques for Memory Forensics, File System Forensics Analysis: NTFS, Ext 2/3/4, FAT, APFS etc., Forensic Study of File System Metadata and Other Attributes, Secure Deletion, Slack Space, Data Recovery.

Unit-3: Computer Forensics

Computer Forensics: Windows Forensics, Data Carving Techniques, Anti and Anti-Anti Forensics, Event Reconstruction Methods and Tools, Time Stomping, Database Forensics, Network Forensics, Approximate Matching.

Unit-4: Emerging Technologies in Digital Forensics

Email Forensics, Mobile Forensics Tools & Techniques, DRONE Forensics, IoT Forensics, Cloud Forensics, Cryptocurrency Forensics, Role of AI in Digital Forensics, AI Forensics, Emerging Technologies in Digital Forensics.

Learning Resources:

Text Books:

1. Eoghan Casey, Handbook of Digital Forensics and Investigation, Academic Press, 2017.
2. Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, III Edition, 2016.
3. Angus McKenzie Marshall, Digital Forensics: Digital Evidence in Criminal Investigations, Wiley-Blackwell, 2018.
4. Carrier, Brian. File System Forensic Analysis. Addison-Wesley Professional, 2005.
5. Computer Forensics and Investigations by Nelson, Phillips Enfinger, Steuart, CENGAGE Learning.
6. Handbook on Securing Cyber-Physical Critical Infrastructure, Sajal K. Das, Krishna Kant, Nan Zhang, Morgan Kaufmann (Elsevier), 2012.
7. Nelson, B, Phillips, A, Enfinger, F, Stuart, C., Guide to Computer Forensics and Investigations, 2nd ed., Thomson Course Technology, 2006.
8. Warren G. Kruse II and Jay G. Heiser, Computer Forensics: Incident Response Essentials, Addison Wesley, 2002.