Minor Stream: Analytics and Security (In Collaboration with Microsoft)

Course Code	Course Name	Level	L	T	P	C	CIE	SEE	Total	Pre-requisite
2501AI36	Network Security Essentials	FC	2			2	50	50	100	-
2501AI37	Introduction to System Design	IC	2		1	3	50	50	100	-
2501AI38	Introduction to Generative AI	IC	2		1	3	50	50	100	-
2501AI39	Cloud Security Essentials	IC	2		1	3	50	50	100	-
2501AI40	Cyber Security Essentials	IC	2		1	3	50	50	100	-
2501AI41	Fundamentals of Block Chain	IC	2		1	3	50	50	100	-
2501AI42	AI for Cyber Threat Intelligence	IC	2		1	3	50	50	100	-
2501AI43	Generative Adversarial Networks Fundamentals	AC	2		1	3	50	50	100	-
2501AI44	AI in Healthcare Security	AC	2		1	3	50	50	100	-
2501AI45	Advanced Topics in Generative AI	AC	2		1	3	50	50	100	-
2501AI46	Ethical AI and Responsible Computing	AC	2		1	3	50	50	100	-
Total			22		**10**	**32**				

Network Security Essentials

	L	T	P	C
Course Code:2501AI36	**2**	**0**	**0**	**2**

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

CO1: Explain fundamental concepts of network security and the need for secure communication.
CO2: Analyze the security aspects of common network protocols and apply standards.
CO3: Configure and use firewalls, VPNs, and IDPS for network protection.
CO4: Implement secure remote access, wireless security, and best practices.
CO5: Use tools for network security monitoring and mitigate DoS/DDoS attacks.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	2	1	1	1	-	-	-	2	-	2
CO2	3	3	2	2	2	-	-	-	2	-	3
CO3	2	3	3	2	3	-	-	-	2	1	3
CO4	2	2	2	2	3	-	-	-	2	2	3
CO5	2	3	3	2	3	-	-	-	2	1	3

Mapping of Course Outcomes with Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	-	2
CO2	-	2
CO3	-	2
CO4	-	2
CO5	-	2

UNIT-I

Introduction to Network Security: Introduction to network security and types of threats, CIA triad and security protocols, firewalls and IDS/IPS systems, antivirus and anti-malware solutions, VPNs and wireless security, access control models and encryption/cryptography, security policies and threat landscape, compliance and regulations, impact of breaches, and remote work with cloud security

UNIT-II

Protocols and Security Standards
TCP/IP stack and DNS resolution, HTTP methods and HTTPS encryption, Packet sniffing and IP spoofing, DNS cache poisoning and man-in-the-middle attacks, TLS/SSL protocols and secure protocol design principles, Firewall, IDS/IPS, and network access control

policies, Port scanning tools (e.g., Nmap) and zero trust architecture, Network security best practices

UNIT-III

Firewalls, VPNs, and IDPS: Stateful vs stateless firewalls and packet filtering, Next-generation firewall (NGFW) and firewall rule configuration, IPSec tunneling protocols and SSL/TLS VPNs, IDS vs IPS and detection methods (signature-based & anomaly-based), Deep packet inspection and zero-day attack detection, VPN encryption protocols and endpoint threat monitoring, Security incident response and network segmentation, Threat monitoring and prevention strategies

UNIT-IV

Wireless and Remote Security: Wi-Fi encryption and rogue access point detection, Evil twin attacks and WIDS, VPN and SSH secure tunneling, SSH key management and brute-force prevention, 2FA/MFA authentication methods, Secure remote access and zero trust, MITM attack prevention and remote desktop security, Endpoint protection and remote endpoint security

UNIT – V

Monitoring, DoS/DDoS & Best Practices:
Network traffic analysis and packet inspection, Intrusion detection and anomaly-based threat detection, Log correlation and SIEM tools, DoS/DDoS mitigation and traffic filtering, Application layer and behavioral attack detection, Access control and least privilege policies, Defense in depth and real-time alerting, Honeypots and deception technologies.

Text Books:

1 Information Security Fundamentals by IBM ICE Publications.
2 Cryptography and Network Security, William Stallings, Pearson Education, 411i Edition
3 Cryptography and Network Security, Atul Kahate, McGrawHill, 2nd Edition

Reference Books:

1 Introduction to Network Security, Neal Krawetz, CENGAGE Learning
2 Information Security, Principles and Practice, Mark Stamp, Wiley India.

Web Links:

1 https://www.geeksforgeeks.org/computer-networks/network-security/
2 https://learn.microsoft.com/en-us/azure/security/fundamentals/network-overview

Introduction to System Design

	L	T	P	C
Course Code: 2501AI37	**2**	**0**	**1**	**3**

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

CO1: Explain system design fundamentals and analyze system requirements.
CO2: Apply core design principles and assess modularity, abstraction, and coupling.
CO3: Compare architectural styles and apply design patterns for system development.
CO4: Design scalable, high-performance systems with optimized data modeling.
CO5: Incorporate security, fault tolerance, and reliability in large-scale system designs.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	3	2	2	1	-	-	-	-	2	2
CO2	3	3	3	1	2	-	-	-	-	1	2
CO3	3	2	3	1	2	-	-	-	-	1	2
CO4	3	3	3	2	3	-	-	-	-	2	2
CO5	3	3	3	2	2	-	-	-	-	2	2

Mapping of Course Outcomes with Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	-	2
CO2	-	2
CO3	-	2
CO4	-	2
CO5	-	2

UNIT-I

System Design Basics & Requirements: System design fundamentals, software architecture patterns, scalability and load balancing, functional and non-functional requirements (NFRs), high availability and fault tolerance, data consistency models and caching strategies, microservices architecture, CAP theorem, security in system design, performance analysis and design for failure

Practice:

1. Define functional and non-functional requirements for an e-commerce system
2. Draw a context-level diagram and requirement document

UNIT-II

Design Principles & Patterns: Object-oriented principles, abstraction in software design, modularity and reusability, encapsulation and information hiding, low coupling and high cohesion, SOLID principles, design pattern catalog (GoF) including Singleton, Factory, Observer, and Strategy patterns, threat modeling in design, secure design principles, anti-patterns and code smells, and design policy enforcement tools

Practice:

1. Implement a modular system using abstraction and encapsulation
2. Apply Singleton and Factory design patterns to a basic problem

UNIT-III

Architectural Styles: Client-server model, layered architecture pattern, monolithic and microservices architecture, service decomposition and inter-service communication (REST/gRPC), scalability and performance trade-offs, deployment complexity and fault isolation, API gateway pattern and load balancing strategies, containerization (Docker/Kubernetes), security risks in distributed systems, service discovery mechanisms, and architecture decision records (ADR)

Practice:

1. Compare microservices and monolithic architectures
2. Design a client-server or layered architecture diagram

UNIT-IV

Database Design & Performance: Database normalization forms, indexing strategies (B-Tree, Hash), entity-relationship modeling and query execution plans, SQL query optimization techniques, read/write load balancing and sharding (horizontal/vertical), in-memory caching (Redis/Memcached) and caching invalidation policies, database partitioning and denormalization trade-offs, data consistency and replication, SQL injection prevention, database performance monitoring tools, and CAP theorem in distributed databases

Practice:

1. Design a normalized schema and ER diagram for a system
2. Analyze index and query optimization for given queries

UNIT – V

Security, Reliability & Case Studies: Security hardening techniques and patch management policies, principle of least privilege with threat modeling and risk assessment, backup and recovery strategies, high availability architecture with redundancy and failover systems, disaster recovery planning with RTO and RPO metrics, SIEM and incident response planning, real-world breach case studies, business continuity planning, cloud-based disaster recovery, and compliance and regulatory requirements (e.g., GDPR, ISO 27001).

Practice:

1. Evaluate a system design for potential security flaws
2. Present trade-offs and analysis from a real-world system case study

Text Books:

1 A. Xu, System Design Interview – An Insider's Guide, ByteByteGo, 2020.
2 M. Kleppmann, Designing Data-Intensive Applications, O'Reilly Media, 2017.
3 M. Richards and N. Ford, Fundamentals of Software Architecture, O'Reilly Media, 2020.

Reference Books:

1 N. Ford and M. Richards, Software Architecture: The Hard Parts, O'Reilly Media, 2021.
2 R. C. Martin, Clean Architecture: A Craftsman's Guide to Software Structure and Design, Pearson, 2017.
3 M. L. Abbott and M. T. Fisher, *The Art of Scalability*, Addison-Wesley, 2015.
4 C. Richardson, Microservices Patterns, Manning Publications, 2018

Web Links:

1 https://www.geeksforgeeks.org/system-design/system-design-tutorial/
2 https://www.ibm.com/docs/en/ram/7.5.4?topic=management-system-design
3 https://nptel.ac.in/courses/107106009

Introduction to Generative AI

Course Code:2501AI38	L	T	P	C
	2	0	1	3

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

CO1: Explain the foundational concepts and types of generative AI models.
CO2: Use Python and libraries like TensorFlow/PyTorch for generative model implementation.
CO3: Prepare and preprocess datasets for effective generative model training.
CO4: Build and evaluate GANs, VAEs, and sequence generation models.
CO5: Apply generative AI to real-world problems and analyze model outcomes.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	2	-	-	2	-	-	-	-	-	3
CO2	3	2	2	1	3	-	-	-	-	-	2
CO3	2	3	2	2	3	-	-	-	-	-	2
CO4	3	3	3	2	3	-	-	-	-	-	2
CO5	2	3	3	3	3	-	-	-	2	1	3

Mapping of Course Outcomes with Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	-	2
CO2	-	2
CO3	-	3
CO4	-	2
CO5	-	2

UNIT-I

Introduction to Generative AI: Generative model fundamentals, GAN architecture and training basics, Variational Autoencoders (VAEs), Autoencoders and representation learning, Sequence generation models (LSTM, GRU), Python syntax and data structures, TensorFlow and PyTorch workflows, Secure and ethical coding practices

Practice:
1. Implement a basic image generator using NumPy
2. Use PyTorch to build a simple autoencoder for MNIST

UNIT-II

Data Preprocessing for Generative Tasks: Data preprocessing and cleaning techniques, Data deduplication and normalization, Data augmentation strategies, Bias and noise

mitigation, Privacy-preserving data processing, Tools for dataset preparation, Dependency and environment management, Ethical data governance and compliance

Practice:

1. Preprocess and augment image data for GANs
2. Preprocess and augment image data for GANs

UNIT-III

Implementation of Generative Models: Generator vs Discriminator roles, Adversarial training loop, Loss functions: Binary Cross, Entropy, Wasserstein, Mode collapse and training challenges, VAE architecture and latent space modeling, Reparameterization trick, Autoencoders: denoising, feature extraction- Implementation using TensorFlow and PyTorch

Practice:

1. Implement a VAE to reconstruct and generate digit images
2. Create a denoising autoencoder and evaluate performance

UNIT-IV

Advanced Generative Architectures: Transformer architecture and pretraining principles, Attention mechanisms and prompt engineering, Language generation and protocol tuning, Overfitting and regularization threats, Bias and fairness in language models, Real-world generative use cases: images, text, healthcare

Practice:

1. Train an LSTM model for character-level text generation
2. Evaluate generative models using FID and Inception Score

UNIT – V

Evaluation, Applications & Ethical Considerations: Inception Score (IS) and FID metrics, Output quality evaluation and benchmarking, Deepfake detection and adversarial risks, Regulatory and compliance policies, Generative AI misuse and ethical risks, Content authenticity and governance, Industry applications and real-world relevance

Practice:

1. Use a pre-trained GPT model for text generation and fine-tuning
2. Develop a mini-project applying generative AI in a selected domain

TextBooks:

1 Ian Goodfellow, Yoshua Bengio, Aaron Courville, *Deep Learning*, MIT Press
2 David Foster, *Generative Deep Learning: Teaching Machines to Paint, Write, Compose, and Play*, O'Reilly
3 Francois Chollet, *Deep Learning with Python*, Manning Publications

Reference Books:

1 PyTorch and TensorFlow official documentation
2 Tutorials from DeepLearning.ai and Coursera on GANs and VAEs
3 Research papers on generative models (NIPS, ICLR, CVPR)

Web Links:

1 https://www.cloudskillsboost.google/course_templates/536
2 https://www.coursera.org/learn/introduction-to-generative-ai

Cloud Security Essentials

Course Code:2501AI39	L	T	P	C
	2	0	1	3

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

CO1: Describe cloud computing concepts and assess cloud-specific security challenges.
CO2: Apply identity and access management strategies including MFA and RBAC.
CO3: Implement encryption, key management, and network security controls in cloud platforms.
CO4: Monitor cloud security events, perform logging, and handle security incidents.
CO5: Evaluate compliance needs and implement governance and cloud security best practices.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	2	2	2	1	1	2	2	-	-	1
CO2	3	3	3	2	2	1	2	2	-	-	1
CO3	3	3	3	2	3	2	1	2	-	-	2
CO4	3	2	3	2	3	2	2	2	-	-	2
CO5	2	2	2	2	2	3	3	3	-	-	3

Mapping of Course Outcomes with Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	-	2
CO2	-	2
CO3	-	1
CO4	-	1
CO5	-	2

UNIT-I

Cloud Security Fundamentals: Cloud service and deployment models, shared responsibility model, identity and access management, cloud access security brokers, data encryption and protection, misconfiguration and API security risks, cloud-native and workload protection tools, compliance frameworks and incident response

Practice:
1. Create a free-tier cloud account and explore services
2. Identify and document shared responsibility for selected services

UNIT-II

IAM and Access Security: Principle of least privilege, Single sign-on (SSO) and identity

providers (IdPs), Role hierarchy and permission sets, Authentication vs authorization, MFA methods and credential protection, OAuth 2.0 and OpenID Connect, Privileged access management (PAM), IAM policies and enforcement

Practice:

1. Create IAM users, roles, and groups in a cloud platform
2. Enable and test MFA for cloud access

UNIT-III

Encryption, Key and Network Security: Encryption techniques and types (AES, RSA, symmetric, asymmetric), Key Management Services (KMS) and key lifecycle, Envelope encryption and HSM, Virtual Private Cloud (VPC) security, Security Groups and NACLs, Firewall types and configurations, VPN and TLS/SSL protocols, Data Leakage Prevention (DLP)

Practice:

1. Encrypt cloud storage with a customer-managed key
2. Set up a secure VPC with firewall and subnet controls

UNIT-IV

Monitoring, Logging and Incident Response: Security logging practices and retention, Log analysis and SIEM integration, Real-time threat detection and response, Incident response lifecycle and automation, Forensic investigation techniques, Security event normalization, Alert tuning and prioritization, Compliance and audit logging

Practice:

1. Enable logging and monitor events in cloud console
2. Simulate and document a simple incident response scenario

UNIT – V

Compliance and Best Practices: Data classification and protection, Compliance frameworks (GDPR,HIPAA,ISO), Cloud governance models, Cloud Security Posture Management (CSPM), Data residency and sovereignty, Encryption and tokenization, Policy enforcement and automation, Risk management and assessment, Data Loss Prevention (DLP), Security best practices in cloud environments.

Practice:

1. Run a compliance check using built-in cloud tools
2. Create a checklist of cloud security best practices

TextBooks:

1 K. Hashizume et al., *An Analysis of Cloud Computing Security Issues*, Springer, 2021
2 G. Reese, *Cloud Application Architectures*, O'Reilly Media, 2009.

3 T. Krutz and R. Dean, *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*, Wiley, 2010

Reference Books:

1 Rittinghouse and J. Ransome, Cloud Computing: Implementation, Management, and Security, CRC Press, 2016
2 B. Grobauer, T. Walloschek, and E. Stöcker, Understanding Cloud Computing Vulnerabilities, IEEE Security & Privacy, 2011
3 D. Linthicum, Cloud Security Basics, O'Reilly Media, 2022

Web Links:

1 https://www.geeksforgeeks.org/software-engineering/cloud-computing-security/
2 https://www.ibm.com/think/topics/cloud-security

Cyber Security Essentials

Course Code:2501AI40	L	T	P	C
	2	0	1	3

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

CO1: Explain core cybersecurity concepts, threat actors, and risk assessment strategies.
CO2: Analyze cyber threats and plan incident responses using appropriate tools.
CO3: Apply cryptographic techniques and secure protocols to protect data in transit and at rest.
CO4: Configure and test technical controls such as firewalls, VPNs, and security infrastructure.
CO5: Implement access control models, conduct penetration testing, and ensure compliance with cybersecurity regulations

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	2	2	2	1	-	-	-	-	-	1
CO2	3	3	3	3	2	-	-	-	1	1	2
CO3	3	3	3	2	2	-	-	-	-	1	2
CO4	3	3	3	3	3	-	-	-	1	2	2
CO5	3	3	3	3	3	-	-	-	2	2	3

Mapping of Course Outcomes with Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	-	2
CO2	-	1
CO3	-	1
CO4	-	2
CO5	-	2

UNIT-I

Foundations of Cybersecurity: CIA Triad and core security principles, Access control and least privilege enforcement, Defense in depth and layered security, Threat actors and malware classification, Social engineering and human factors, Risk assessment and incident response, Security tools and endpoint protection, Cybersecurity frameworks and awareness training

Practice:
1. Research recent cyber attacks and present threat types,
2. Simulate a phishing or fake login page for awareness

UNIT-II

Web Security and Cryptography: OWASP Top 10 vulnerabilities, Injection attacks (SQL, Command), Broken authentication, Sensitive data exposure, HTTPS and TLS

protocols, TLS handshake process, Symmetric encryption (AES), Asymmetric encryption (RSA), Hashing algorithms (SHA-256), Digital signatures and integrity, Public Key Infrastructure (PKI), SSL/TLS certificate validation, Secure key management, Cryptographic attack vectors (brute force, padding oracle), Secure coding best practices

Practice:

1. Perform OWASP web vulnerability testing using Juice Shop or Burp Suite,
2. Capture and analyze HTTPS traffic using Wireshark.

UNIT-III

Access Control and IAM: Discretionary Access Control (DAC), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Identity and Access Management (IAM), Multi-Factor Authentication (MFA), Single Sign-On (SSO), Authentication vs Authorization, OAuth 2.0 protocol, OpenID Connect, Identity Federation, Credential theft prevention, Privileged Access Management (PAM), Identity lifecycle management, Access control policies, Insider threat mitigation

Practice:

1. Configure MFA and role-based access control in a demo web app,
2. Set up and manage user identities using OpenLDAP

UNIT-IV

Technical Controls and Infrastructure: Network intrusion detection systems (NIDS), Network intrusion prevention systems (NIPS), Virtual Private Networks (VPN) protocols (IPSec, SSL/TLS), Firewall rule configuration, Next-generation firewalls (NGFW), Deep packet inspection (DPI), Traffic monitoring tools (Wireshark, Zeek), Port scanning and enumeration (Nmap), Secure tunneling protocols, Access control lists (ACLs), Bandwidth and anomaly analysis, Zero Trust Network Architecture, Threat intelligence integration, Security logging and alerting, Network segmentation and isolation

Practice:

1. Set up a basic firewall using UFW or pfSense
2. Configure a VPN connection and verify encryption

UNIT – V

Compliance, Ethics, and Auditing: General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), Data privacy principles and data minimization, Digital rights and ethical hacking, Security compliance frameworks and continuous compliance monitoring, Risk assessment, mitigation and third-party risk management, Security audit processes, governance and legal implications of cyber threats and breach notification policies, Privacy Impact Assessments (PIA)

Practice:

1. Conduct a mock compliance audit (GDPR, HIPAA, etc.)
2. Draft a simple security policy for a small organization

Text Books:

1 W. Stallings, Network Security Essentials: Applications and Standards, Pearson, 2016
2 M. Whitman and H. Mattord, Principles of Information Security, Cengage Learning, 2021
3 C. P. Pfleeger and S. L. Pfleeger, Security in Computing, Pearson, 2015

Reference Books:

1 M. Sikorski and A. Honig, Practical Malware Analysis, No Starch Press, 2012
2 S. Malik, Security Operations Center: Building, Operating, and Maintaining Your SOC, Apress, 2020
3 T. Holt et al., Cybercrime and Digital Forensics: An Introduction, Routledge, 2018
4 R. Bejtlich, The Practice of Network Security Monitoring, No Starch Press, 2013

Web Links:

1 https://www.coursera.org/learn/cyber-security-fundamentals
2 https://learn.microsoft.com/en-us/training/paths/describe-basic-concepts-of-cybersecurity/

Fundamentals of Block Chain

Course Code:2501AI41	L	T	P	C
	2	0	1	3

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

CO1: Explain the foundational concepts of blockchain and distributed systems
CO2: Demonstrate cryptographic techniques and consensus mechanisms used in blockchain
CO3: Develop smart contracts and deploy decentralized applications
CO4: Identify real-world blockchain use cases and evaluate their feasibility
CO5: Analyze blockchain limitations, trends, and regulatory concerns

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	2	-	-	2	-	-	-	-	-	3
CO2	3	3	2	2	3	-	-	-	-	-	2
CO3	3	2	3	2	3	-	-	-	2	2	2
CO4	2	3	2	2	3	-	-	-	2	2	3
CO5	2	3	2	2	2	-	-	-	3	2	3

Mapping of Course Outcomes with Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	-	2
CO2	-	2
CO3	-	2
CO4	-	3
CO5	-	3

UNIT-I

Introduction to Blockchain: Consensus algorithms, Blockchain models, Cryptographic hashing, Block creation and validation, Node synchronization, Smart contracts, Scalability and security in decentralized systems, Blockchain applications and compliance

Practice:
1. Simulate a basic blockchain with chained blocks and hash computation
2. Implement SHA-256 and verify hash changes with block data

UNIT-II

Cryptographic Foundations: Symmetric and asymmetric cryptography, Cryptographic hash functions, Digital signatures and PKI, Key management and trust models, Cryptanalysis and security threats, Consensus protocols (PoW vs PoS), Data confidentiality and integrity, Quantum-safe and regulatory-compliant cryptography

Practice:

1. Demonstrate digital signatures and key pair generation using Python
2. Set up a local Ethereum blockchain using Geth

UNIT-III

Smart Contracts and Platforms: Ethereum architecture and EVM, Solidity programming and contract deployment, Gas optimization and DApp design, Smart contract security and tools (Remix, Truffle), Blockchain oracles and integrations, Hyperledger Fabric and chaincode, Consensus mechanisms and access control (MSP), Enterprise blockchain scalability and interoperability

Practice:

1. Develop and deploy a simple smart contract using Solidity in Remix
2. Connect a smart contract to frontend using Web3.js and MetaMask

UNIT-IV

Blockchain Use Cases: DeFi and cross-border payments, Blockchain in supply chain and logistics, Healthcare privacy and EHR systems, Secure voting and digital identity (SSI), IoT authentication and data integrity, NFT standards, ownership, and provenance, Regulatory compliance and cybersecurity risks, Cross-platform blockchain interoperability

Practice:

1. Explore real-world blockchain use case – land registry or supply chain
2. Deploy an ERC-20 token or NFT (ERC-721) on testnet

UNIT – V

Challenges & Future Trends: Layer 2 scaling solutions, blockchain interoperability, regulatory compliance and legal frameworks, smart contract security, Web3 identity and access control, DeFi risks and vulnerabilities, protocol optimization and composability, tokenomics and governance

Practice:

1. Analyze transaction data and gas fees on Ethereum testnet
2. Present current trends in blockchain (e.g., Web3, Layer 2, DeFi, ZK-rollups)

TextBooks:

1 Imran Bashir, *Mastering Blockchain*, Packt Publishing
2 Melanie Swan, *Blockchain: Blueprint for a New Economy*, O'Reilly Media
3 Andreas M. Antonopoulos, *Mastering Ethereum*, O'Reilly Media

Reference Books:

1 Arvind Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, Princeton University Press

2 Joseph Bonneau et al., *SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies* (IEEE)
3 Hyperledger Fabric documentation – https://hyperledger-fabric.readthedocs.io/

Web Links:

1 https://learn.microsoft.com/en-us/shows/beginners-series-to-blockchain/
2 https://learn.microsoft.com/en-us/archive/msdn-magazine/2018/march/blockchain-blockchain-fundamentals

AI for Cyber Threat Intelligence

Course Code:2501AI42	L	T	P	C
	2	0	1	3

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

CO1: Describe AI concepts and their application to cyber threat intelligence
CO2: Build ML models for threat detection, anomaly detection, and alert classification
CO3: Apply NLP and deep learning for malware and phishing analysis
CO4: Automate CTI tasks such as incident response and SOC operations using AI
CO5: Analyze limitations, adversarial threats, and ethics in AI-driven security systems

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	2	1	2	-	-	-	-	-	-	2
CO2	3	3	3	2	1	-	-	-	-	1	2
CO3	3	3	3	2	1	-	-	-	-	-	2
CO4	3	2	3	2	-	-	-	-	-	2	2
CO5	2	2	2	2	-	-	-	-	-	-	2

Mapping of Course Outcomes with Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	-	2
CO2	-	2
CO3	-	2
CO4	-	2
CO5	-	2

UNIT-I

Introduction to AI in Cybersecurity: Cyber Threat Intelligence (CTI) lifecycle, threat intelligence types (tactical, operational, strategic), threat actor profiling and TTPs, indicators of compromise (IoCs), threat modeling and risk assessment, AI/ML in threat detection, threat data enrichment and correlation, threat intelligence platforms and protocols (STIX, TAXII), threat hunting and incident response integration, automation and policy-based mitigation

Practice:
1. Explore threat intelligence feeds and IoC extraction

UNIT-II

ML Techniques for Threat Detection: Supervised and unsupervised learning for threat

detection, clustering and classification models (K-Means, DBSCAN, SVM, Random Forest), feature extraction and selection in cybersecurity, DDoS and insider threat detection using ML, time-series analysis for threat detection, reducing false positives and evaluating models (precision, recall, F1), real-time intrusion detection with ML, adversarial machine learning threats, data labeling challenges, and integration of ML models into SIEM and security policy enforcement

Practice:

1. Build a supervised ML model to detect phishing URLs
2. Perform anomaly detection using clustering on network logs

UNIT-III

NLP and Deep Learning in Threat Intelligence: Phishing detection using NLP, Malware behavior analysis via text mining, Log parsing and normalization, Threat intelligence report mining, Named entity recognition in cybersecurity texts, Word embeddings for threat classification, RNNs for sequential log analysis, CNNs for network traffic classification, Transformer models in cybersecurity, Semantic analysis of threat reports, Protocol anomaly detection using deep learning, NLP-based spam and phishing email filtering, Tokenization and feature extraction from logs, Policy compliance through log analysis, Cyber threat hunting using deep neural networks

Practice:

1. Use NLP to extract threats from CTI reports
2. Classify malware samples using CNN models

UNIT-IV

Automated Threat Intelligence and SOC Integration: SIEM architecture and data pipelines, Real-time threat detection and correlation, Alert fatigue and triage optimization, Risk-based case prioritization, Playbook automation for incident response, MITRE ATT&CK integration with SIEM, Threat intelligence enrichment in alerts, Anomaly detection in security events, Reinforcement learningfor adaptive defense, Autonomous incident response systems, Policy-driven alert classification, Behavioral analytics for SOC operations, Protocol-aware event normalization, Threat scoring using machine learning, Modern SOAR-SIEM integration

Practice:

1. Automate alert triage using AI on SIEM data
2. Simulate incident response workflow with intelligent decision trees

UNIT – V

Challenges, Ethics, and Adversarial AI: Adversarial example generation techniques, Model poisoning and data integrity threats, Evasion attacks in deployed ML models,

Explainable AI for security decision-making, Differential privacy in model training, Secure federated learning protocols, AI model auditing and risk assessment, Robustness evaluation metrics for ML models, Regulatory frameworks for AI security (e.g., EU AI Act), Privacy-preserving machine learning, Secure multi-party computation in AI, Threat modeling for ML systems, Policy compliance in AI model deployment, Detection and mitigation of AI supply chain attacks, Interpretable ML tools for SOC analysts

Practice:

1. Evaluate model robustness against adversarial attacks
2. Use explainable AI (XAI) to interpret threat model decisions
3. Present a case study on real-world AI threat intelligence system

Text Books:

1 Sumeet Dua and Xian Du, *Data Mining and Machine Learning in Cybersecurity*, CRC Press
2 Clarence Chio and David Freeman, *Machine Learning and Security*, O'Reilly Media
3 Nina Godbole and Sunit Belapure, *Cybersecurity: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*, Wiley

Reference Books:

1 MITRE ATT&CK Framework – https://attack.mitre.org/
2 IBM X-Force Exchange – https://exchange.xforce.ibmcloud.com/
3 Research papers on adversarial ML in cybersecurity (IEEE/ACM)

Web Links:

1 https://learn.microsoft.com/en-us/credentials/certifications/cybersecurity-architect-expert/

Generative Adversarial Networks Fundamentals

	L	T	P	C
Course Code:2501AI43	**2**	**0**	**1**	**3**

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

CO1: Explain the architecture, components, and purpose of GANs.
CO2: Implement various types of GANs using TensorFlow or PyTorch
CO3: Apply GANs to tasks like image generation, style transfer, and image translation.
CO4: Evaluate advanced GAN techniques and their applications
CO5: Identify ethical implications and limitations associated with GANs.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	2	2	2	1	1	-	1	-	-	1
CO2	3	3	3	3	3	1	-	-	-	-	2
CO3	3	3	3	3	3	1	1	-	-	-	2
CO4	3	3	3	3	2	2	1	-	-	-	2
CO5	2	2	2	1	1	3	2	3	1	-	2

Mapping of Course Outcomes with Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	-	2
CO2	-	1
CO3	-	1
CO4	-	2
CO5	-	2

UNIT-I

Foundations of GANs: Generative Adversarial Networks (GANs), Generator vs Discriminator and adversarial training, GAN loss functions and mode collapse, DCGAN and Conditional GANs (cGAN), CycleGAN and StyleGAN architectures, TensorFlow and PyTorch GAN implementations, Dataset preparation and evaluation metrics (FID, IS), Ethical concerns, security threats and responsible AI guidelines

Practice:

1. Train a Deep Convolutional GAN (DCGAN) to generate new images and check its quality.
2. Generate class-specific images with cGAN and try unpaired image translation using CycleGAN.

UNIT-II

Basic GANs and Conditional GANs: Basic GAN implementation and architecture design, Adversarial loss functions and training stability, Conditional GANs and label conditioning, Dataset labeling and preprocessing techniques, Mode collapse prevention and generalization, GAN training with TensorFlow/PyTorch, Evaluation metrics (FID, IS) and output analysis, Use cases of cGANs (image-to-image, data augmentation), Ethical concerns, deepfake detection, and content regulation policies

Practice:

1. Build a simple GAN to generate images, watch training behavior, and try one fix for mode collapse.

UNIT-III

DCGANs, CycleGANs and PGGANs: DCGAN design and convolutional architecture, Normalization and activation strategies, CycleGAN for unpaired image translation, Generator consistency and domain transfer, Progressive GANs and resolution scaling, Training stability and GAN frameworks, Synthetic data risks and authenticity challenges, Ethical AI use and policy development.

Practice:

1. Build a DCGAN to generate images, learn normalization/activation choices, then try a simple progressive upscaling (PGGAN-lite) to improve resolution

UNIT-IV

Style GANs and Applications: StyleGAN architecture and improvements, Latent space and style manipulation, GANs for data augmentation and imbalance handling, Anomaly detection using GANs, GAN frameworks (PyTorch/TensorFlow), Synthetic data risks and adversarial robustness, Deepfake detection and misuse prevention, Ethical governance and explainability of GAN outputs

Practice:

1. Generate a few images using a pretrained StyleGAN generator, perform a small latent interpolation, and discuss possible applications, risks, and ethics.

UNIT – V

Ethics and Advanced Techniques: Deepfake generation and detection, Privacy and ethical risks of synthetic data, GAN training challenges (convergence issues, mode collapse, evaluation), Advanced GAN architectures (WGAN-GP, SAGAN, BigGAN), AI-generated content regulations, Bias and fairness in GAN outputs, Content authenticity and verification, Governance and responsible AI frameworks

Practice:

1. Learn how deepfakes are detected, why they're risky, and how policy/ethics guide safe work.
2. Implement a small WGAN-GP (or adapt a given tiny implementation), observe training stability and mode collapse, and test for bias in generated outputs. Propose governance / mitigation steps.

Text Books:

1 Goodfellow et al., Deep Learning, MIT Press, 2016
2 A. Rosebrock, Deep Learning for Computer Vision with Python, PyImageSearch, 2019
3 I. Goodfellow, Y. Bengio, and A. Courville, Generative Adversarial Networks, MIT Deep Learning Series, 2020

Reference Books:

1 J. Brownlee, Generative Adversarial Networks with Python, Machine Learning Mastery, 2021
2 S. Li and L. Wand, Progressive Growing of GANs for Improved Image Synthesis, arXiv preprint, 2018
3 A. Brock et al., Large Scale GAN Training for High Fidelity Natural Image Synthesis, ICLR, 2019
4 H. Zhang et al., Self-Attention Generative Adversarial Networks, ICML, 2019

Web Links:

1 https://developers.google.com/machine-learning/gan/gan_structure
2 https://www.geeksforgeeks.org/deep-learning/generative-adversarial-network-gan/

AI in Healthcare Security

Course Code:2501AI44	L	T	P	C
	2	0	1	3

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

CO1: Explain the role of AI in healthcare security and data protection
CO2: Analyze healthcare data security standards and regulatory frameworks.
CO3: Apply AI methods like ML, NLP, and generative models to detect and prevent threats
CO4: Design privacy-preserving AI systems for healthcare environments
CO5: Evaluate healthcare security incidents and propose AI-driven compliance solutions.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	2	2	2	2	2	-	-	-	-	2
CO2	3	3	3	3	3	1	-	-	-	-	3
CO3	3	3	3	2	2	3	-	-	-	1	2
CO4	3	2	2	2	1	3	-	-	-	1	2
CO5	2	2	2	1	1	2	-	-	-	2	2

Mapping of Course Outcomes with Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	-	2
CO2	-	1
CO3	-	1
CO4	-	2
CO5	-	2

UNIT-I

Introduction to AI in Healthcare Security: AI-driven threat detection, data privacy and HIPAA compliance, anomaly detection in patient data, encryption and access control protocols, Zero Trust architecture in healthcare, cybersecurity policies and governance, ransomware and phishing threats, privacy-preserving machine learning, real-time monitoring and alerting tools

Practice:

1. Analyze anonymized healthcare datasets and identify data privacy issues

UNIT-II

Healthcare Data Security and Regulatory Frameworks: HIPAA Security Rule, PHI encryption protocols, access control and authentication, data breach threats, compliance

monitoring tools, risk management frameworks, regulatory enforcement and penalties, cloud and mobile security challenges, privacy policies and audit requirements

Practice:

1. Implement HIPAA-compliant data handling procedures in AI workflows

UNIT-III

Core AI Techniques in Healthcare Security: Threat intelligence platforms, anomaly detection algorithms, behavioral analysis, zero-day threat response, data encryption standards (AES, RSA), key management protocols, intrusion detection systems (IDS), cloud data protection, AI-driven threat identification

Practice:

1. Train a supervised ML model for malware detection in healthcare
2. Use NLP to detect phishing or fraud in medical communication logs
3. Perform threat intelligence extraction using ML from threat reports

UNIT-IV

Advanced AI Models and NLP in Healthcare Security: Generative Adversarial Networks (GANs), Variational Autoencoders (VAEs), synthetic data generation, anonymization techniques, privacy-preserving AI, differential privacy, deepfake detection, model inversion attacks, supervised learning for fraud detection, insider threat identification using NLP, AI-powered communication monitoring tools

Practice:

1. Build a generative model (GAN) for synthetic medical data
2. Configure access control and network security for a simulated hospital network
3. Evaluate the impact of adversarial attacks on healthcare AI systems

UNIT – V

Cybersecurity Operations and Compliance in Healthcare: Intrusion detection and prevention systems (IDPS), Endpoint Detection and Response (EDR), RBAC/ABAC, multi-factor authentication (MFA), SIEM tools, adversarial ML threats, model robustness, fairness and bias mitigation, forensic analysis, GDPR principles, AI-driven compliance monitoring, automated auditing protocols, post-incident review and modern breach prevention strategies

Practice:

1. Analyze a real-world healthcare breach and propose AI solutions
2. Build a dashboard for compliance monitoring using AI tools

Text Books:

1 Pascal Hitzler et al., *Foundations of AI in Healthcare*, Springer
2 Sumeet Dua and U. Rajendra Acharya, *Machine Learning in Healthcare Informatics*, Springer
3 HIPAA Journal – https://www.hipaajournal.com/

Reference Books:

1 Arvind Narayanan et al., *Security and Privacy in Machine Learning*, Princeton University Resources
2 Research papers from IEEE, Springer, Elsevier on AI in healthcare cybersecurity
3 OWASP Healthcare InfoSec resources – https://owasp.org/

Web Links:

1 https://www.microsoft.com/en-us/research/project/ai-for-health/

Advanced Topics in Generative AI

	L	T	P	C
Course Code:2501AI45	**2**	**0**	**1**	**3**

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

CO1: Explain the architectures and working of advanced GenAI models
CO2: Implement and fine-tune generative models for practical applications
CO3: Analyze and create multimodal generative systems
CO4: Evaluate ethical, legal, and societal implications of GenAI technologies
CO5: Design solutions using prompt engineering and domain-specific generative pipelines.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	2	2	2	2	1	2	2	-	-	2
CO2	3	3	3	3	3	2	1	-	-	-	3
CO3	3	3	3	3	3	1	2	-	1	-	2
CO4	2	2	2	2	1	3	3	3	1	-	2
CO5	3	3	3	3	3	1	2	2	1	-	3

Mapping of Course Outcomes with Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	-	2
CO2	-	1
CO3	-	2
CO4	-	2
CO5	-	2

UNIT-I

Architectures in Generative AI: Generative Adversarial Networks (GANs), Variational Autoencoders (VAEs), Autoregressive models (PixelCNN, WaveNet), Denoising Diffusion Probabilistic Models (DDPM), Latent diffusion models (LDMs), Transformer-based text generation, GPT architecture and applications, T5 for text-to-text tasks, BERT for masked language modeling and generation, Ethical concerns in generative AI, Misuse of synthetic content, Hallucination and bias in AI models, Content authenticity and watermarking, Open-source vs closed-source model policies, Responsible AI development frameworks

Practice:
1. See differences between a VAE and a small DCGAN on MNIST
2. Generate text with a small GPT model and check for hallucinations / bias.

UNIT-II

Training & Fine-tuning GenAI Models: Pretraining vs fine-tuning paradigms, Transfer learning in NLP, Prompt tuning techniques, Prompt injection attacks, Prompt engineering best practices, Reinforcement Learning with Human Feedback (RLHF), Human-in-the-loop training, Model alignment and safety, Low-Rank Adaptation (LoRA), Parameter-Efficient Fine-Tuning (PEFT), Model robustness and adversarial prompts, Ethical considerations in LLM training, Bias and fairness in fine-tuning, Secure deployment of tuned models, Governance policies for generative AI

Practice:

1. See the difference between full fine-tuning and lightweight prompt-based tuning on a small NLP task
2. Understand how prompt injection can make an LLM ignore instructions and learn basic mitigation

UNIT-III

Multimodal Generative AI: Text-to-Image generation (DALL·E, Stable Diffusion), Text-to-Audio synthesis (e.g., Bark, Tortoise TTS), Text-to-Video models (e.g., Sora, Gen-2), Diffusion models in multimodal generation, Latent space conditioning, Image captioning algorithms, Visual Question Answering (VQA) systems, Multimodal Transformers (e.g., Flamingo, GPT-4V), Cross-modal embedding techniques, Ethical concerns in synthetic media, Deepfake detection in multimodal content, Dataset biases in multimodal training, Content moderation policies, Accessibility through multimodal AI, Responsible deployment of generative models

Practice:

1. Generate images from text prompts using a pretrained diffusion model (Stable Diffusion mini / DALL·E API) and then generate captions for them using a pretrained image-captioning model.
2. Ask a pretrained Visual Question Answering (VQA) model questions about an image and check for biases or incorrect answers.

UNIT-IV

Applications and Industry Use Cases: AI-assisted content creation tools (e.g., Canva, Adobe Firefly), Generative design in digital media, AI in code generation (e.g., GitHub Copilot, CodeWhisperer), Game development with generative AI, Personalized learning with AI tutors, AI in medical imaging and diagnostics, Drug discovery using generative models, AI for scientific hypothesis generation, Responsible AI in education and healthcare, Data privacy in GenAI applications, Intellectual property and content ownership, Bias and fairness in AI-generated content, Human-AI

Practice:

1. Use a free AI-assisted tool (like Canva Text-to-Image or Adobe Firefly free plan) to create designs from text prompts and reflect on ownership, bias, and real-world use.
2. Use an AI code assistant (GitHub Copilot, CodeWhisperer, or Hugging Face CodeGen) to generate solutions for small problems, test outputs, and discuss

safety/privacy.

UNIT – V

Ethical Considerations and Governance: Deepfakes and synthetic media threats, Disinformation and misinformation campaigns, AI alignment challenges, Bias in training data and model outputs, Hallucination in generative AI models, Content authenticity verification, Model interpretability and explainability, Copyright issues in AI-generated content, Legal frameworks for AI governance, International AI regulations (EU AI Act, U.S. EO), Ethics in AI development and deployment, Responsible AI and GenAI frameworks (e.g., OECD, NIST), Safety protocols for model deployment, Transparency and accountability in GenAI, Human oversight and control in AI systems

Practice:

1. Explore how deepfakes/synthetic media can be created and detected, and discuss the risks and governance measures.
2. Understand bias in model outputs and the importance of explainability & governance.

Text Books:

1 Goodfellow et al., Deep Learning, MIT Press, 2016
2 L. Hugging Face Team, The Transformers Book, Hugging Face, 2023
3 A. Radford et al., Language Models are Few-Shot Learners, OpenAI, 2020
4 P. Isola et al., Image-to-Image Translation with Conditional Adversarial Networks, CVPR, 2017

Reference Books:

1 C. Raffel et al., Exploring the Limits of Transfer Learning with a Unified Text-to-Text Transformer, JMLR, 2020
2 OpenAI, GPT-4 Technical Report, arXiv, 2023
3 A. Dosovitskiy et al., An Image is Worth 16x16 Words: Transformers for Image Recognition at Scale, ICLR, 2021
4 C. O'Neil, Weapons of Math Destruction, Crown Publishing, 2016

Web Links:

1 https://www.coursera.org/courses?query=generative%20ai
2 https://learn.microsoft.com/en-us/training/modules/fundamentals-generative-ai/

Ethical AI and Responsible Computing

	L	T	P	C
Course Code:2501AI46	**2**	**0**	**1**	**3**

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

CO1: Explain the ethical foundations and societal impact of AI and computing
CO2: Identify algorithmic bias, discrimination, and fairness concerns in AI systems
CO3: Apply ethical frameworks and principles to assess AI design and deployment
CO4: Design responsible AI solutions adhering to transparency and accountability
CO5: Analyze legal, regulatory, and real-world challenges in AI ethics.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	2	3	2	-	1	-	-	-	-	2	2
CO2	2	2	2	-	1	-	-	-	-	-	1
CO3	2	3	2	-	1	-	-	-	-	2	2
CO4	3	3	1	-	-	-	-	-	-	-	2
CO5	3	3	1	-	-	-	-	-	-	1	1

Mapping of Course Outcomes with Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	-	2
CO2	-	2
CO3	-	2
CO4	-	2
CO5	-	2

UNIT-I

Introduction to Ethical AI: Algorithmic bias,AI transparency and explainability, Ethical hacking and penetration testing, Data privacy and consent, Deepfake and misinformation threats, Responsible AI principles, Digital surveillance ethics, Ethical governance frameworks, AI policy and regulatory compliance

Practice:

1. Analyze ethical dilemmas in emerging AI use cases

UNIT-II

Bias and Fairness in AI: Algorithmic bias detection, Fairness metrics evaluation, Discrimination in automated decisions, Bias mitigation techniques, Ethical AI principles, Fairness-aware machine learning tools, Regulatory and policy frameworks, Inclusive data practices, Real-world case studies of algorithmic bias

Practice:

1. Identify bias in datasets and explore fairness metrics

UNIT-III

Ethical Frameworks and Principles: Ethical decision-making frameworks, AI moral reasoning models, Deontological rule-based systems, Utilitarian outcome optimization, Virtue ethics in AI behavior, Human-centered design principles, Value alignment in AI systems, Ethical risk assessment protocols, Policy guidelines for ethical AI

Practice:

1. Evaluate AI algorithms using ethical impact assessment tools
2. Conduct an ethical risk analysis on a public AI system

UNIT-IV

Responsible AI Design: Explainability techniques in AI, Model interpretability tools, Accountability in automated decisions, Transparency principles in AI systems, Auditing protocols for AI models, Ethical threats of black-box algorithms, Regulatory policies for XAI, Human-in-the-loop frameworks, Trust and reliability in AI outputs

Practice:

1. Design an interpretable AI model and generate explanations using XAI
2. Develop a code of ethics or policy guideline for responsible AI use

UNIT – V

Governance, Policy, and Regulation: EU AI Act provisions, Global AI regulatory frameworks, Data privacy and protection laws, Compliance auditing tools, Risk-based AI classification, Legal and ethical AI principles, Enforcement protocols for AI governance, Cross-border data sharing threats, Challenges in regulatory compliance

Ethical Challenges in Real-world Applications: Biometric data protection, AI surveillance ethics, Deepfake detection technologies, Autonomous decision-making protocols, Privacy threats in facial recognition, Regulatory frameworks for AI surveillance, AI misuse and societal impact, Security vulnerabilities in AV systems, Legal and ethical governance of deepfakes

Practice:

1. Simulate a case study review under AI regulation (e.g., GDPR or EU AI Act)
2. Explore adversarial impacts of unregulated AI systems (e.g., misinformation, surveillance)
3. Debate a controversial AI deployment and propose ethical alternatives

TextBooks:

1 Virginia Dignum, *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way*, Springer

2 Markus D. Dubber, Frank Pasquale, Sunit Das, *Oxford Handbook of Ethics of AI*, Oxford University Press
3 Shannon Vallor, *Technology and the Virtues: A Philosophical Guide to a Future Worth Wanting*, Oxford University Press

Reference Books:

1 IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems
2 World Economic Forum – AI Governance Frameworks
3 AI Now Institute Reports – https://ainowinstitute.org/

Web Links:

1 https://www.microsoft.com/en-us/ai/responsible-ai#:~:text=Microsoft's%20responsible%20AI%20principles%20include,inclusiveness%2C%20transparency%2C%20and%20accountability.