NED University of Engineering & Technology

Department of Computer Science & Information Technology

MS (Information Security)
Course Catalogue

MS in Information Security

Programme structure

Students have to complete thirty (30) credit hours in MS (IS) programme. There will be four customized non-credit courses (pre-requisites) only for candidates coming from fields other than computer science/engineering and software engineering), five (05) compulsory courses and five (05) elective courses of three (03) credit hours each.

S.No	Course No.	Customised Courses Course Title	Credit Hrs
1	CT-491	Operating System	NC
2	CT-492	Object Oriented Programming	NC
3	CT-493	Data Structure and Algorithm Design	NC
4	CT-494	Introduction to Databases	NC

S.No	Course No.	Compulsory Courses Course Title	Credit Hrs
1	CT-506	Advanced Analysis of Algorithms	3
2	CT-508	Cryptography	3
3	CT-509	Distributed Systems	3
4	CT-539	Advanced Computer Networking	3
5	CT-574	Information Privacy and Security	3

S.No	Course No.	Elective Courses Course Title	Credit Hrs
1	CT-507	Wireless and Mobile Communication Networks	3
2	CT-532	Information System Audit	3
3	CT-541	Network Security	3
4	CT-542	Information Security Management	3
5	CT-543	Database Security	3
6	CT-544	Cyber Crimes and Security	3
7	CT-545	Digital Forensics	3
8	CT-546	Secure E-Commerce	3
9	CT-547	Secure Programming	3
10	CT-548	Security Testing Theory and Practice	3
11	CT-549	Multimedia Security and Privacy	3

12	CT-550	Trusted Computing	3
13	CT-551	Fault Tolerance and Reliability	3
14	CT-552	Quantum Cryptography	3
15	CT-553	Emerging Trends in Information Security	3
16	CT-554	Ethical Hacking	3
17	CT-555	Cloud Security	3
18	CT-556	Intrusion Detection	3
19	CT-557	Privacy Engineering	3
20	CT-558	Distributed Blockchain Technologies	3
21	CT-571	Nature Inspired Optimisation Algorithms	3
23	SE-512	Research Methodology	NC
22	CT-5002	Thesis	6

Course Content

[Customized Courses]

CT-491 : Operating System

Course Content

- Operating System Overview: Objectives and Functions
- Processes: States, Description, Control
- Processor Scheduling: Types & Algorithms, Multiprocessor & Real-Time Scheduling.
- Threads, SMP and Microkernels
- Concurrency – Principles; Mutual Exclusion (Software Approaches, Hardware Support, Operating System Support)
- Concurrency: Deadlock and Starvation
- Memory Management: Requirements, Virtual Memory.
- I/O Management and Disk Scheduling - I/O Function Organization,
- Operating, System Design Issues; I/O Buffering; Disk Buffering
- File Management: Organization and Access;
- Directories; Sharing; Record Blocking; Secondary Storage Management
- Protection and Security: Computer Security;
- Trusted Systems; Network Security; Viruses and Related Threats.
- Client-Server or Microkernel Operating Systems.
- Networking and Distributed Processing - Communication Architecture; Servers;
- Process Migration; Distributed Process Communication.

CT-492 : Object Oriented Programming

Course Content

- Introduction to Programming Languages.
- Introduction to Programming.
- Object Oriented Programming OOP.
- Objects & Classes.
- Introduction to UML.
- Class diagrams and Use cases.
- Passing object by arguments.
- Constructors and Destructors.
- Copy Constructor.
- Function Overloading
- Visual Development and Event-Driven Programming
- Static Variables and Static member functions.
- Returning Objects from a function.
- Unary Operator Overloading.
- Binary Operator Overloading.
- Single level Inheritance.
- Multilevel Inheritance.
- Multiple Inheritance.
- Hybrid Inheritance.
- Hierarchical Inheritance.
- Containership.

- Virtual functions.
- Pure virtual functions and abstract classes.
- Reading and writing a text file.
- Reading and writing a binary file.
- Filing.

CT-493 : Data Structure and Algorithms Design

Course Content

- Data Structures: Fundamental concepts, Arrays, Stacks, Queues, Priority Queues, Linked Lists, Trees, Spanning Trees, Graphs and Traversals.
- Recursion, sorting and searching algorithms, Shortest path algorithms, Storage and retrieval properties and techniques for various data structures.
- Algorithms Analysis Fundamentals: Induction, Recurrence relations, Big-Oh and little-Oh notation, Merge sort.
- Graph Algorithms: Depth-first search, strongly connected components, Breadth-first search, Dijkstra's algorithm
- Greedy Algorithms: Minimum spanning tree
- Union find, Set cover, Huffman coding
- Dynamic Programming: Longest common subsequence, Traveling salesman.
- Divide and Conquer: Integer multiplication, Matrix multiplication
- Hashing: Balls into bins problems, Bloom filters
- Document similarity.

CT-494 : Introduction to Databases

Course Content

- Database concepts.
- Database Architecture.
- DB Design Life Cycle.
- Schema Architecture.
- Conceptual, logical and physical database modeling and design.
- Entity Relationship Diagram (ERD). Enhanced ERD.
- Relational data model.
- Mapping ERD to relational model. Functional dependencies and
- Normalization.
- Relational Algebra.
- Structured Query language (SQL).
- Transaction processing.
- Concurrency control and recovery techniques.
- Query optimization concepts.
- Emerging Trends in Database:
- Introduction to On-Line Analytical Processing (OLAP).

Course Content

[Compulsory Courses]

CT-506 : Advanced Analysis of Algorithms

Course Content

- Introduction of formal techniques and the underlying mathematical theory.
- NP-completeness; Search Techniques;
- Randomized Algorithms.
- Heuristic and Approximation Algorithms.
- Asymptotic analysis of upper and average complexity bounds using Big-O, little-o, and theta notation.
- Fundamental algorithmic strategies (brute -force, greedy, divide-and-conquer, backtracking, branch-and-bound, pattern matching, and numerical approximations).
- Standard graph and tree algorithms.
- Additional topics: standard complexity classes, time and space tradeoffs in algorithms, using recurrence relations to analyze recursive algorithms, non-computable functions, the halting problem, and the implications of non-computability.

CT-508 : Cryptography

Course Content

- Cryptography history and classification.
- Elementary number theory: Prime numbers, Factoring, Modular arithmetic, Fermat's & Euler's theorems, gcd, Euclid's algorithm, Discrete logarithm problem.
- Block ciphers: Block cipher principles, Feistel networks, S boxes and P boxes, Block cipher modes of operation, DES, 3DES, AES.
- Hash digests: Properties of cryptographic hash functions, Merkle Damgard construction, md family, sha family, Digital signatures, sha3
- Stream Ciphers: Linear Feedback Shift Register (LFSR), RC4.
- Public key encryption: Public key crypto systems, RSA algorithm, Elliptic Curve cryptography.
- Interactive Proofs, Zero-Knowledge Proofs, Zero-Knowledge Proofs of Knowledge, Non-Interactive Zero-Knowledge Proofs, Secure Protocols, Two-Party Secure Computation, Multiparty Secure Computation, Chosen Cipher text Security.

CT-509 : Distributed Systems

Course Content

- Application challenges: mobile systems; sensor networks; ubiquitous/pervasive computing; peer-to-peer computing; overlay networks; mobile networks; distributed data mining.
- System challenges: communication mechanisms; processes; naming synchronization; data storage and access; consistency and replication; fault-tolerance; security.
- Coupling: platform; temporal and spatial; bus and broker architecture styles; review of Web services; service oriented architectures (SOA); SOA building blocks; software as a service.
- Utility computing: on-demand computing; Grid computing; Cloud computing; Autonomic computing; case studies.

CT-539 : Advanced Computer Networking

Course Content

- Introduction and Classification of Computer networks.
- OSI & TCP/IP reference model and design issues.
- Transmission media.
- Data Link Layer Implementation Issues and Protocols.
- Medium Access Control: Static & Dynamic Allocation Techniques.
- ATM Technology.
- Synchronous Optical Network (SONET/SDH)
- Broadband Networks.
- HDLC Protocol: Point-to-point Protocol (PPP).
- Multiple Access Protocol: WIFI (802.11); Implementation issue & Frame Architecture
- Multiple Access Protocol: Ethernet (802.3); Implementation issue & Frame Architecture
- Access Technology: Orthogonal Frequency Division (OFDM.)
- Multiple Access Protocol: WIMAX (802.16) Implementation Issue, Frame Format & Architecture.
- Voice over IP (VoIP).
- Topics from Emerging Technologies in Computer Networking.

CT-574 : Information Privacy and Security

Course Content

- Overview of e-security: Threats, risks, consequences, Sources of threats, Attacks classification, Preventive measures, remedial measures.
- Cryptography for e-security: Historical perspective, Confusion vs. diffusion, Stream ciphers vs. block ciphers, Keys and key management, Key exchange (peer to peer, peer – key server – peer), Diffie Helman key sharing scheme, Symmetric key cryptography vs asymmetric key cryptography, Trapdoor functions.
- GPG: Overview of GPG, Commands and CLI, GPG trust model, GUI – KGPG, Seahorse, Frontends – Kleopatra, enigmail.
- Practical applications: PKI, CA. X509 certificates, SSL/TLS, HTTPS, IPV6 and IPSEC, Proxies and Firewalls.
- Misc. techniques: Encryption using non-cryptographic tools (vi, zip), Authentication principles and methods, Passwords, two-factor authentication, One-way encryption, Steganography, Hamming, Chaffing and Winnowing.
- Management aspects: System Administration policies, Security audit, Penetration testing and ethical hacking, Mandatory Access control, Discretionary Access Control, Monitoring and logging tools, Legal aspects.

Course Content

[Elective Courses]

CT-507 : Wireless and Mobile Communication Networks

Course Content

- Overview of wireless communications. Cellular wireless networks, Generations of cellular networks, Wireless local area networks (Wi-Fi), Mobile IP.
- Mobile ad hoc networks (MANET).
- Wireless personal area networks (Bluetooth, UWB, ZigBee), Wireless sensor networks.
- Wireless technologies design and evaluation, Handoff management, Location management, Resource management, Network and service management and control, Energy management and efficiency of protocols and devices
- Cognitive radio networking, Device-to-device communications, Routing and scheduling in mobile and wireless networks, Transport layer issues in mobile and wireless networks.
- Network security solutions and protocols, Subscriber privacy, Authentication, Authorization, Accounting, Traffic and network modeling.
- Analysis, and simulation in wireless/mobile networks - Virtualized and cloud-based wireless.
- Simulations of wireless networks.

CT-532 : Information System Audit

Course Content

- The Process of Auditing Information Systems: Risk-based IT audit strategy, Specific audit planning, IT audit standards, Audit reporting, communications and follow-up.
- Governance and Management of IT Domain: IT governance structures, IT organizational structure and HR, IT strategy and direction, IT policies, standards and procedures, QMS and IT management of controls, Monitoring and assurance practices, IT resource management, IT contracting strategies and policies, Risk management practices, Business continuity planning (BCP)
- Information Systems Acquisition, Development and Implementation: Business case development, Project management practices, Project reviews, Develop project controls, Information systems implementation and migration, Post implementation reviews.
- Information Systems Operations, Maintenance and Support: Information systems reviews, Service level management practices, Third-party management practices, End-user procedures and operations, Maintenance of information systems, Data administration practices, Capacity and performance monitoring, Problem and incident management, Change, configuration and release management, Backup and restoration of systems.
- Protection of Information Assets: Information security policies, standards and procedures and generally accepted practices. Design, implementation and monitoring of system and logical security controls to verify confidentiality, integrity, availability

CT-541 : Network Security

Course Content

- Basic concepts in network security.
- Role of Cryptography in Network Security: Cyphers, Role of Cryptography in Information Security (Secret key and public key cryptosystems including RSA, DSA, Diffie-Hellman key exchange), one-way hash function.
- Network Architectures: Architecture Development, Network Security Models, Security Capabilities of Networking Protocols
- Network Based Attacks: General Attacks, Attacks on Layers 1 and 2, Network Based Attacks on Layer 3, Network Based Attacks on Layer 4, Network Based Attacks on Applications.

- Network Element Security: Network Security within Operating Systems and Applications and Network Infrastructure Components
- Network Layers 1 and 2 Security Mechanisms: Media types, 802.1q, 802.1X, 802.11, Sonet, (G)MPLS
- Network Layer 3 Protocol Security Mechanism: IPsec and examples
- Network Layer 3 Device Security Mechanisms: Packet Filtering (Stateless & Statefull Firewalls, Application Gateways) and Deep Packet Inspection (Intrusion Detection, Intrusion Prevention), Flow Detection
- Network Layer 4 Security Mechanisms: TLS, DTLS, SSL, SSH, Malware, Security Certification.
- Security in ad-hoc networks, Recent advances in network security.

CT-542 : Information Security Management

Course Content

- Information Security Management Principles: Concepts and Definitions, The Need for, and the Benefits of Information Security.
- Information Security Framework: Organization and Responsibilities, Legal Framework, Security Standards and Procedures. Security models. IS 27001 - Information Security Management for Business Benefit. Internal Control, Audit and Security.
- Information Risk: Threats to, and Vulnerabilities of Information Systems, Risk Management. Risk analysis and CRAMM.
- Technical Security Controls: Protection from Malicious Software, Networks and Communications, External Services. Cloud Computing. IT Infrastructure.
- Software Development and Lifecycle: Testing, Audit and Review, Systems Development and Support
- Business continuity planning – a safety net for business, Building an information security, management framework.
- Information Security, Governance and the Law. The Business of Trust.

CT-543 : Database Security

Course Content

- Introduction: Security issues faced by enterprises.
- Database Management Systems: RDMS, query processing, normalization, Transaction management, Recovery.
- Database Security Overview: General security issues, Access control models.
- Security Architecture: Database Security, User Admin, Profiles, Passwords etc. Database Security Models, Database Auditing, Transaction Processing.
- Serialisability Theory, Two Phase Locking. Centralized Recovery, Distributed Recovery, DB Security Models.
- Relational Database Security. Statistical Database Security. Concurrency Control and Multi-Level Security.
- Database auditing models, Application data auditing, Practices of database auditing, Security of commercial relational databases.
- Distributed Databases: Design Issues, Distributed query processing, Transaction management, Distributed concurrency control, Reliability, Data integration, Data replication
- Security issues: Security policies, Identity management, Integrity and availability, MLS architecture, SOA and Cloud data management, Secure stream data management.

CT-544 : Cyber Crimes and Security

Course Content

- Introduction: Types of computer crime, history, surveys, statistics and global connections.
- Legal Measures: Computer Misuse, Criminal Damage, Software Piracy, Forgery, Investigative Powers.
- Case Studies: Investigations into hacking, cases and PC misuse.
- Social Engineering.
- Spam, Phishing and Pharming.
- Malware: The types, effects, and investigations.
- DoS and Distributed DoS: The causes, mechanisms, case studies, and countermeasures.
- Network Crimes: Hacking methodologies via the Internet and attacks to other networks
- Investigations, incident handling and forensic examination.
- The Future: Identity Theft and Fraud.
- Networks and dependencies; Critical infrastructures and interdependencies;
- Security of Cyber-Physical Systems; Control systems security;
- Advanced persistent threats; Attack modelling techniques;
- System assurance; Incident response mechanisms;
- Offensive cyber operations; Future challenges.

CT-545 : Digital Forensics

Course Content

- Introduction to forensic science,
- steps from collecting data to preserving evidence, and a framework for digital forensic evidence collection and processing
- Context: Legal and Practical Considerations
- Cybercrime; Forensic process; Legal process and law enforcement; ACPO guidelines; Digital evidence; Incident response.
- Computer Forensics: File Systems, (File system organisation; Memory; Registry; System logs); Disk imaging; Programs and their traces; Searching and analysis; Investigative tools (Open Source and Proprietary); Email & Browsers, Fundamentals of host forensics for different operating systems MS Windows, Unix / Linux etc.
- Foundations of network forensics: Intrusion detection; Attack trace-back; Packet inspection; Log analysis.
- Steganography techniques for images, video, textual data, and audio. Mobile devices, Games consoles, etc.; Hashing issues; Anti-forensics (encryption and stealth techniques).
- A survey of non-standard storage mechanisms from retention characteristics to mobile and smart phones and vehicular systems as well as network-based search and storage mechanisms.

CT-546 : Secure E-Commerce

Course Content

- The importance of e-commerce security to the business enterprise.
- Current threats facing organizations that conduct business online and how to mitigate these challenges.
- Cryptography review.
- Public key certificates and infrastructures, authentication and authorization

- Introduction and implementations on secure web based application development using various technologies such as XML, Perl, PHP, ASP, JSP and JavaScript.
- Cryptographic tools to support confidentiality, integrity, authentication, digital signature, non-repudiation services for electronic transmissions and transactions.
- Public Key Infrastructure (PKI) and Certificate Authorities and X.509 standard
- Security Schemes: IPSec, SSL, Kerberos, PGP and SET
- Secure credential services and role-based authorization,
- Mobile code security,
- Security of agent-based systems,
- Secure electronic transactions,
- Electronic payment systems,
- Intellectual property protection,
- Law and Regulation.

CT-547 : Secure Programming
Course Content

- Security maintenance of deployed software systems, including "penetrate-and patch", vulnerability enumeration (CVE IDs) and classification (CWE taxonomy).
- Secure programming techniques and common pitfalls, covering input validation, output filtering, use of cryptography and authentication. Secure Coding Standards.
- Malware and its use of software vulnerabilities as an attack vector. Programming resilience against malware.
- Low-level programming platforms, VMs and their security provisions, Mobile operating system platforms
- Web programming platforms and security provisions. HTTP protocol, forms, client-side and server-side threats and their avoidance.
- High-level and Enterprise security programming
- Security APIs and their distinction from cryptography APIs. Use and design of security APIs for key management, hashing and encryption.
- Language-based techniques for assisting security programming, using dynamic enforcement via runtime monitoring and static enforcement via program analysis.
- Methods and tools for taint checking and information flow tracking to manage programming with sensitive data. Privacy risks with lack of encapsulation.
- Methods and tools for controlling resource usage with permissions.

CT-548 : Security Testing Theory and Practice
Course Content

- Introduction to security testing, legal aspects of penetration testing, standards and certification.
- Security testing frameworks and methodologies, and how to prepare, manage and conduct a professional penetration testing.
- Technical aspects of network security covering standards, protocols, routing, firewalls showing the theoretical basis of vulnerabilities and how these may be exploited in practice.
- Technical aspects of computer security covering operating systems, access control in windows and linux/unix, host based intrusion detection, escalation of privileges and how to exploit these vulnerabilities in practice and how to harden systems.
- Technical aspects of Internet based applications, web services, protocols, languages (e.g. SQL) and how these may be exploited using for example SQL injection and cross- site scripting; how to exploit these vulnerabilities in practice, and how to harden the applications.

- A survey of non-standard and emerging technologies and review of potential threats these may lead to.

CT-549 : Multimedia Security and Privacy
Course Content

- Introduction to Digital Rights Management (DRM) and Digital Watermarking and Multimedia Security
- Models of Watermarking, Basic Message Coding, Error Correction Coding.
- Theoretic Aspects of Digital Watermarking, Mutual Information and Channel Capacity, Information Theoretical Analysis of Digital Watermarking.
- Digital Watermarking Schemes: Spread Spectrum Watermarking, DCT-Domain Watermarking, Quantization Watermarking, A Buyer-Seller Watermarking Protocol, An Efficient and Anonymous Buyer-Seller Watermarking Protocol
- Media-Specific Digital Watermarking: Video Watermarking, Audio Watermarking, Binary-Image Watermarking
- Advanced Digital Watermarking: Watermarking with Side Information, Improved Spread Spectrum, Robustness to Temporal and Geometric Distortions
- Affine-Resistant Watermarking
- Steganography and Steganalysis
- Introduction to Digital Right Management Products and Laws.
- Fingerprinting and Digital Forensics.
- Non-Intrusive Digital Forensics.
- Cryptography and Multimedia Encryption.
- Privacy-Preserving Data Mining and Clustering.
- Data Sanitization, Privacy-Preserving Surveillance.

CT-550 : Trusted Computing
Course Content

- Computer security – an overview of current challenges, Cryptography basics,
- Trusted computing concepts.
- Privacy in Trusted Computing and DAA; Single Sign-on, Secure delivery of conditional access applications, Securing peer-to-peer networks using trusted computing.
- Security Models: Intro to modern crypto and security models/arguments,
- Pseudorandom Functions, Symmetric Encryption, Hash Functions, Message Authentication, Asymmetric Encryption, Oblivious Transfer and Secure Function Evaluation, The Random Oracle Model
- The Trusted Software Stack, TPM Keys, Secure Storage, Secure identification
- Administration of Trusted Devices.
- Privacy and Direct Anonymous Attestation.
- Virtualization and Trusted Computing.
- Advanced topics – latest issues in Trusted Computing.
- Virtual Monotonic Counters and Applications, TPMs for instantiating random oracles, TPMs for non-interative OT and SFE.

CT-551 : Fault Tolerance and Reliability

Course Content

- Need for reliability: Faults as the sources of unreliability; anticipated and unanticipated faults; fault prevention and fault tolerance approaches to achieving reliability.
- System dependability concepts and terminology: failures, error, design and component faults.
- Fault tolerance: principles, error detection, damage assessment, error recovery, fault treatment; redundancy; TMR systems; programming with exception and exception handlers.
- Error detection: Ideal measures for error detection; replication checks; timing checks; coding checks.
- Error recovery: Forward and backward error recovery; their advantages and limitations; implementation issues in backward error recovery; co-operating processes and recovery lines.
- Software fault tolerance: N-version programming, recovery blocks.
- Hardware fault tolerance: fault classification and replication strategies; need for agreement among replicas; evaluation of redundancy requirements.
- Case studies Mars, Delta-4.

CT-552 : Quantum Cryptography

Course Content

- Mathematical background: Linear algebra
- Basic concepts: Postulates of Quantum Mechanics, Qubit, Qubit representation in
- Bloch Sphere, Basis, Orthogonal basis; Orthonormal basis, Mutually unbiased bases
- Information transfer via qubits. No Cloning Theorem.
- Intercept-resend eavesdropping strategy. Quantum Key Distribution and its security.
- QKD Protocols: BB84, B-92, SARG-04.
- High error-rate Quantum Key Distribution Protocols. Evaluation of Quantum Key Distribution protocols.
- Entanglement based QKD protocols,
- Quantum Key Distribution Networks.
- Applications of Quantum Cryptography in Classical Computer Networks.
- Post-quantum cryptography. Position-based quantum cryptography.

CT-553 : Emerging Trends in Information Security

Course Content

- This course covers a wide range of topics in information security including security protocols (models, properties, and verification), and contemporary security issues in emerging applications in e-commerce, e-voting, social networking and e-health etc. Selected topics will reflect the nascent development and trends of interest in the area of information security.

CT-554 : Ethical Hacking

Course Content

- Introduction to Ethical Hacking
- Technical foundation of cracking and ethical hacking
- Aspects of security, importance of data gathering, Footprinting, Reconnaissance and system hacking
- Scanning Networks
- Enumeration
- System Hacking
- Trojans and Backdoors
- Viruses, Worms and Sniffers

- Social Engineering
- Session Hijacking
- Hacking Webservers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- Evading IDS, Firewalls, and Honeypots
- Buffer Overflow
- Evaluation of computer security
- Penetration Testing

CT-555 : Cloud Security
Course Content

- Cloud computing and its deployment models, Virtualization Security, Hypervisor security,
- NIST Cloud Computing Security Reference Architecture
- Cloud Security Alliance (CSA) Model for Cloud Security
- Top Security Challenges to Cloud Computing by CSA
- Network Security in Cloud Computing
- Data Privacy and Trust challenges in Cloud Computing,
- Cloud Data Centre Security,
- Denial of Service attacks in Cloud and their mitigations,
- Identity management in Cloud Computing
- Homomorphic Encryption
- Cryptographic Key Management in Cloud Computing
- Auditing in Cloud,
- Security as a Service Model

CT-556 : Intrusion Detection
Course Content

- Intrusion Detection Concepts and History
- Intrusion Detection System (IDS) Products and Components
- IDS Monitored Platforms: Host-Based IDS, Network-Based IDS, Hybrid IDS
- Attack detection methods: Signature-Based Detection, Statistical Anomaly detection, Statefull Protocol Analysis Detection
- IDS Deployment Architectures: Non-distributed and distributed
- Evaluation of Intrusion Detections Systems
- Intrusion Detection and Prevention Systems (IDPS)
- Limitations of IDS
- Evasion techniques
- Advanced topics: Intrusion Detection in Virtual Networks, Clouds, IoT and other modern applications.

CT-557 : Privacy Engineering

Course Content

- Introduction to privacy,
- Conceptual Framework for understanding Privacy
- Web Privacy: Online Tracking
- Detecting Data Use on the Web:
- Privacy Design Strategies
- Privacy Preserving Computation
- Searchable Encryption
- Privacy Preserving Data Mining
- Privacy Enhancing Technologies (PETs),
- The Right of Privacy in the age of Digital Networks
- Database Privacy,
- Data Perturbation Techniques
- Privacy in Healthcare: HIPAA
- Privacy Policy, Law and Technology
- Social Networking and Privacy
- Privacy Compliance in Big Data Systems

CT-558 : Distributed Blockchain Technologies

Course Content

- Blockchain Foundations: The Brief History of Blockchain, The Move to Decentralization, Ledgers, Distributed Ledgers, and Consensus.
- Technical background of blockchain: Cryptography, Hash Functions, Public Key Cryptography and Signing, Blocks and Blockchain, the Chain, Nodes and Network.
- Trust Framework and Consensus Mechanisms, Public, Consortium, Private Blockchains, Blockchain Interoperability, When to Use a Blockchain (Limitations and Misconceptions), Implications of Blockchain on Traditional Business.
- Bitcoin and Ethereum, Smart Contracts, Cryptocurrency Tokens, Wallets and the Marketplaces, and Implications on Traditional Businesses.
- Applications: Self-Sovereign Identity and Reputation, Ownership and Governance, Supply Chain and Asset Tracking.

CT-571 : Nature Inspired Optimisation Algorithms

Course Content

- Heuristics and Metaheuristic,
- Optimization,
- Single-objective vs. Multi-objective optimization,
- Multi-objective optimization methods,
- Genetic algorithms,
- Simulated Evolution,
- Stochastic Evolution,
- Simulated Annealing,
- Ant colony optimization,
- Particle Swarm optimization,
- Honeybee colony optimization,
- Cuckoo search,

- Extremal optimization,
- Latest Nature-inspired iterative algorithms,
- Advanced concepts (Hybridization, Hyper-heuristics etc.)