M.Tech. in CSE (with Specialization Cyber Security)

IIITDM Kurnool and CRRao AIMSCS

Semester-1

Course Code	**Course Name**	**Credits**
CY501	Mathematical Foundation for Cyber Security	3 (3-0-3)
CY502	Advanced Data Structures and Algorithms	5 (3-3-5)
CY504	Computer Systems	5 (3-3-5)
CY505	Modern Cryptography	5 (3-3-5)
CY5XX	Elective-1	3 (3-0-3)
CY594	Technical Presentation	2 (0-3-2)
	Total	**23**

Electives-1

Basket-1		**Basket-2**	
CY551	Data Privacy	CY561	Intelligent Systems
CY552	Cloud Computing	CY562	Unmanned Aerial Vehicle
CY553	Wireless Networked Systems	CY563	Machine Learning
CY554	Mobile Computing	CY564	Artificial Intelligence
CY555	Quantum Computing	CY565	Natural Language Processing
CY556	Post Quantum Cryptography		

Semester-2

Course Code	**Course Name**	**Credits**
CY511	Web and Network Security	5 (3-3-5)
CY512	Cloud and IoT Security	5 (3-3-5)
CY513	Ethical Hacking & Computer Forensics	5 (3-3-5)
CY514	Cyber Crime, Cyber Laws & IPR	3 (3-0-3)
CY5YY	Elective-2	3 (3-0-3)
CY595	Professional Writing	2 (0-3-2)
		23

Electives-2

Basket-1		**Basket-2**	
CY571	Quantum Cryptography	CY581	Information System Control and Audit
CY572	Security of Cyber Physical Systems	CY582	Machine Learning Applications for Cyber Security
CY573	Blockchain Technology	CY583	Incident Response and Threat Intelligence
CY574	Secure Coding	CY584	Social Network Analysis
		CY585	Image security
		CY586	Secure Machine learning
		CY587	Secure GIS systems

Cumulative credit of the course

Semester	Subject	Credits	
1	Semester-I	23	
2	Semester -II	23	
3	Semester - III Project and Thesis - 1 *	12	
4	Semester -IV Project and Thesis - 2 *	12	
		70	

* Students are allowed either in IIITDM Kurnool or in CRRao AIMSCS for their final year project

Mathematical Foundations for Cyber Security

Prerequisite: Nil **Credit:** 3-0-3

Course Objectives:

1. To develop the students' ability to use mathematical concepts, methods, and tools that are applicable to Cyber Security
2. To help the students understand the importance of mathematics in computer science and its use in computer science applications
3. To develop the students' ability to apply mathematical concepts and techniques to solve Cyber Security problems
4. To enable the students to learn the foundations of discrete mathematics and its applications in computer science and cyber security

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

1. Ability to use the mathematical concepts in the field of Cyber Security
2. Employ the techniques and methods related to the area of Cyber Security in variety of applications
3. Apply logical thinking to understand and solve the problem in context
4. Analyze and design computer algorithms based on mathematical concepts and reasoning
5. Apply mathematical concepts to programming languages and software systems

Detailed Syllabus:

Cyber Security Fundamentals: What is Cyber Security? Why is it important? Cyber security goals: Confidentiality, Integrity, Availability.

Algebra: Group, Permutation Groups, Cosets, Normal Subgroups, Group Homomorphisms, Group Isomorphisms, Ring, Field, Finite fields.

Linear Algebra: Matrices and their properties (determinants, traces, rank, nullity, etc.); Eigenvalues and eigenvectors; Matrix factorizations; Inner products; Distance measures; Projections; Notion of hyperplanes; half-planes.

Mathematical Logic and Proofs: logical operators, statements and propositions, truth tables, tautologies and logical equivalences, formal proof methods such as direct proof, proof by contradiction, proof by induction.

Probability and Statistics: Probability theory and axioms; Random variables; Probability distributions and density functions (univariate and multivariate); Expectations and moments; Covariance and correlation; Statistics and sampling distributions.

Textbooks:

1. G. Strang . Introduction to Linear Algebra, Wellesley-Cambridge Press, Fifth edition, USA, 2016.
2. Bendat, J. S. and A. G. Piersol. Random Data: Analysis and Measurement Procedures. 4th Edition. John Wiley & Sons, Inc., NY, USA, 2010
3. Joseph A. Gallian, Contemporary Abstract Algebra, Brooks/Cole Pub Co Publisher, 8th Edition, 2012.

Reference books:

4. Montgomery, D. C. and G. C. Runger. Applied Statistics and Probability for Engineers. 5th Edition. John Wiley & Sons, Inc., NY, USA, 2011.
5. David G. Luenberger . Optimization by Vector Space Methods, John Wiley & Sons (NY), 1969.
6. Cathy O’Neil and Rachel Schutt . Doing Data Science, O’Reilly Media, 2013.

Advanced Data Structures and Algorithms

Prerequisite - NIL **Credit:** 3-3-5

Course Objectives:

1. To learn to analyze and design efficient algorithms which work with improved data structures
2. To understand the theoretical concepts of advanced data structures and algorithms
3. To develop an understanding of the applicability of data structures and algorithms in computer science and engineering
4. To learn to evaluate the efficiency of algorithms and data structures

Course Outcomes:

1. Understand the implementation of symbol table using hashing techniques
2. Apply advanced abstract data type (ADT) and data structures in solving real world problem
3. Effectively combine the fundamental data structures and algorithmic techniques in building a solution to a given problem
4. Develop algorithms for text processing applications
5. To communicate physics concepts and their applications to engineering fields effectively.

Detailed Syllabus:

Dictionaries: Definition, Dictionary Abstract Data Type, Implementation of Dictionaries, Hashing: Review of Hashing, Hash Function, Collision Resolution Techniques in Hashing, Separate Chaining, Open Addressing, Linear Probing, Quadratic Probing, Double Hashing, Rehashing, Extendible Hashing Skip Lists: Need for Randomizing Data Structures and Algorithms, Search and Update Operations on Skip Lists, Probabilistic Analysis of Skip Lists, Deterministic Skip Lists,

Trees: Binary Search Trees (BST), AVL Trees, Red Black Trees: Height of a Red Black Tree, Red Black Trees Bottom-Up Insertion, Top-Down Red Black Trees, Top-Down Deletion in Red Black Trees, Analysis of Operations 2-3 Trees: Advantage of 2-3 trees over Binary Search Trees, Search and Update Operations on 2-3 Trees, Analysis of Operations,

B-Trees: Advantage of B- trees over BSTs, Height of B-Tree, Search and Update Operations on 2-3 Trees, Analysis of Operations, Splay Trees: Splaying, Search and Update Operations on Splay Trees, Amortized Analysis of Splaying

Text Processing: Sting Operations, Brute-Force Pattern Matching, The Boyer-Moore Algorithm, The Knuth-Morris-Pratt Algorithm, Standard Tries, Compressed Tries, Suffix Tries,

The Huffman Coding Algorithm, The Longest Common Subsequence Problem (LCS), Applying Dynamic Programming to the LCS Problem, Computational Geometry: One Dimensional Range Searching, Two Dimensional Range Searching, Constructing a Priority Search Tree, Searching a Priority Search Tree, Priority Range Trees, Quadtrees, k-D Trees

Text books:

1. Mark Allen Weiss, Data Structures and Algorithm Analysis in C++, second Edition, Pearson, 2004

Reference books:

1. T.H. Cormen, C.E. Leiserson, R.L.Rivest, Introduction to Algorithms, Third Edition Prentice Hall, 2009
2. Michael T. Goodrich, Roberto Tamassia, Algorithm Design, First Edition, Wiley, 2006

Computer Systems

Prerequisite: Operating systems and computer networking **Credit:** 3-3-5

Course Objectives:

1. Understand the architecture and organization of computer systems.
2. Understand the functions of operating systems and their role in managing computer resources.
3. Understand the principles of distributed systems and client-server architecture.
4. Understand the concepts of concurrency and synchronization in multi-process and multi-threaded systems.
5. Understand the principles of computer security and protection.

Course Outcomes:

1. Analyze the performance metrics of computer systems and evaluate their suitability for different applications.
2. Design and implement simple operating system components such as process scheduling algorithms and memory management algorithms.
3. Design and implement distributed systems using client-server architecture and remote procedure call mechanisms.
4. Analyze and solve concurrency and synchronization issues in multi-process and multi-threaded systems using locking mechanisms, semaphores, monitors, and condition variables.
5. Students can evaluate the security and protection mechanisms in operating systems and design secure and robust systems.

Detailed Syllabus

Introduction to Computer Systems, Overview of computer hardware and software, Role and purpose of computer systems, Computer architecture and organization, Performance metrics of computer systems, Operating Systems Fundamentals, Definition and functions of an operating system, Types of operating systems, Process management and scheduling, Memory management and virtual memory, Input/output management, File systems and storage management.

Distributed Systems and Client-Server Architecture, Definition and characteristics of distributed systems, Comparison of distributed systems with centralized and decentralized systems, Client-server architecture and its components, Remote procedure call, message-oriented middleware, Sockets and network programming.

Distributed file systems and naming services, Process and Thread Synchronization, Concurrency and synchronization issues in multi-process and multi-threaded systems, Mutual exclusion and locking mechanisms, Semaphores, monitors, and condition variables, Deadlock and starvation prevention and avoidance, Thread-level parallelism and synchronization, Security and Protection in Operating Systems, Threats to operating system security, Access control and protection mechanisms, Authentication and authorization.

Cryptography and secure communication, Security protocols and policies, Case Studies and Emerging Trends, Case studies of operating systems and distributed systems, Emerging trends in operating systems and computer systems.

Reference books:

1. "Computer Systems: A Programmer's Perspective" by Randal E. Bryant and David R. O'Hallaron
2. "Computer Security: Principles and Practice" by William Stallings and Lawrie Brown
3. "Operating System Concepts" by Abraham Silberschatz, Peter B. Galvin, and Greg Gagne
4. "Distributed Systems: Principles and Paradigms" by Andrew S. Tanenbaum and Maarten van Steen

Modern Cryptography

Prerequisite - NIL **Credit: 3 - 3 - 5**

Course Objectives:

- Provide a solid mathematical foundation in cryptography
- Explore both symmetric (private-key) and asymmetric (public-key) encryption techniques, focusing on their construction, security guarantees, and limitations.
- Familiarize students with key cryptographic algorithms, including DES, AES, RSA, El Gamal, and Elliptic Curve Cryptography (ECC), along with associated security models and attack vectors.
- Study the construction, application, and vulnerabilities of cryptographic hash functions, message authentication codes (MACs), and digital signatures for secure communication.
- Examine advanced cryptographic techniques like secret sharing, zero-knowledge proofs, and commitment schemes, and understand their real-world applications.
- Connect theoretical cryptography with practical implementations to enable students to build and evaluate secure systems in real-world contexts.

Course Outcomes:

- Understand key cryptographic concepts such as modular arithmetic, Fermat's Little Theorem, and Euler's Theorem.
- Analyze symmetric encryption schemes (DES, AES) and understand CPA-security and the construction of secure encryption.
- Understand cryptographic hash functions, MACs, and their vulnerabilities (e.g., birthday attacks).
- Learn about public-key encryption schemes (RSA, El Gamal) and the Diffie-Hellman protocol.
- Study digital signature schemes (Schnorr, DSA, Elliptic Curve DSA) and understand their security in PKI.
- Learn about Secret Sharing Schemes, commitment schemes, and Zero Knowledge Proof systems.

Course: PG Level

Syllabus

Module - 1

Course Overview, Mathematical background: Modular Inverse, Extended Euclid Algorithms, Fermat's Little Theorem, Euler Phi-Function, Euler's theorem. Modular arithmetic, Inverses, Fermat's Little Theorem, Euler's Theorem, Chinese Remainder Theorem, Prime numbers and primality testing.
Historical Ciphers, Stream Ciphers. Perfectly-Secret Encryption: Definitions, the one-time pad; proven limitations.

Private-Key (Symmetric) Encryption: Computational security, Defining and Constructing secure encryption; Constructing CPA-secure encryption,

Module - 2
Data Encryption Standard (DES), Triple DES, Man-in-the-middle attack, Advanced Encryption Standard (AES). Provably secure Instantiation of PRG, Practical Instantiation of PRG, CPA-Secure Ciphers from PRF, Modes of Operations of Block Ciphers. Message Authentication Codes (MAC), Information-theoretic Secure MAC, Cryptographic Hash Functions. Birthday Attacks on Cryptographic Hash Functions, Applications of Hash Functions.

Module - 3
Discrete-Logarithm Problem, Computational Diffie-Hellman Problem, Decisional Diffie-Hellman Problem, Elliptic-Curve Based Cryptography and Public-Key Encryption, El Gamal Encryption Scheme, RSA Assumption, CCA - secure Public-key Hybrid Ciphers Based on Diffie-Hellman Problems and RSA-assumption.

Module - 4
Digital Signatures: Schnorr Signature and its security, Digital-signature Standard Algorithm (DSA), Elliptic Curve DSA, Boneh-Lynn-Shacham Signature and its security. Certificate Management, Public Key Infrastructure (PKI).

Module - 5
Secret Sharing Scheme, (t, n)-Shamir Secret Sharing Scheme, Commitment Scheme and its security definition. Pedersen Commitment Scheme. Interactive Proof Systems and Zero Knowledge Proof systems.

References

1. Jonathan Katz and Yehuda Lindell, Introduction to Modern Cryptography, Chapman and Hall/CRC publication, 2nd edition, 2014.
2. Douglas R. Stinson and Maura Paterson, Cryptography: Theory and Practice, Chapman and Hall/CRC publication, Standard Edition, 2018.
3. A. Menezes, P. Van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, 2004.
4. Behrouz A. Forouzan, Introduction to Cryptography and Network Security, Mc Graw Hill Publication, 2020.
5. Mike Rosulek. The Joy of Cryptography

Online Courses (Similar to this course)

1. NPTEL Foundations of Cryptography, By Dr. Ashish Choudhury, IIIT Bangalore, https://nptel.ac.in/courses/106106221.
2. Cryptography, by Prof Don Boneh, Stanford University https://www.coursera.org/learn/crypto.

Technical Presentation

Prerequisite: NIL **Credit:** 0-3-2

Course Objectives:

1. Demonstrate an understanding of the importance of technical writing in Computer Science and Engineering
2. Develop effective technical writing skills such as writing precise and clear instructions, reports and proposals
3. Effectively use computer-based tools for writing, research and formatting
4. Identify and apply a variety of technical writing styles
5. To develop research and presentation skills

Course Outcomes:

1. Analyze the selected topic, organize the content and communicate to audience in an effective manner
2. Write standard technical documents like reports, proposals and articles
3. Use appropriate citation methods for technical documents
4. Create stunning visual aids (e.g. graphics and diagrams)
5. Employ well-tested editing and formatting techniques

Detailed Syllabus

Technical Writing and its scope Classroom Activity: Group discussions with brief presentations; Overview of Technical writing genres (Reports, Proposals, Instructions and User Manuals). Classroom Activity: Industry reports and proposal analysis; Business and Technical writing principles Classroom Activity: Analyzing principles of effective technical Writing; Language Standards and Editing Techniques Classroom Activity: Peer review and editing assignments; Technical Writing tools (Software and Platforms) Classroom Activity: Real-time practice with software tools; Graphics and Visual Aids Classroom Activity: Practical exercises in creating graphical representations;

Web and Network Security

Prerequisite: NIL **Credit**: 3-3-5

Course Objectives:

1. To introduce the foundational principles of web and network security, including threats, vulnerabilities, and risk management strategies.
2. To explain and analyze authentication and access control models, enabling students to design secure identity and authorization mechanisms.
3. To provide an in-depth understanding of perimeter security technologies, such as firewalls, IDS/IPS, and DMZ configurations, for evaluating network defenses.
4. To equip students with hands-on knowledge of securing routers and network devices, focusing on their configuration as security components.
5. To study cryptographic protocols including PKI and digital certificates, and explore host hardening techniques for protecting systems against common cyberattacks.

Course Outcomes:

1. .Design of Access Control and Authentication mechanisms for security
2. Evaluate and Appraise the perimeter security fundamentals
3. Create and Assemble the router security to set it up as a security device
4. Understand and Describe PKI security protocols and Digital Certificate
5. Assess and Evaluate host hardening for various attacks.

Course Structure:

UNIT I

Securing Information Using Authentication and Access Control: introduction to Access Control, Implementing an Authentication Strategy, Implementing an Access Control Strategy, Cryptography, PKI: Introduction to Certificates, Introduction to Public Key Infrastructure, Deploying and Managing Certificates

UNIT II

Perimeter Security Fundamentals, Packet Filtering: How packet filtering works, Problems with packet filters, Dynamic packet, Stateful firewalls: How stateful firewall works, The concept of a state, Stateful inspection and stateful filtering,

UNIT III

Proxy firewalls: Proxy or application gateway firewalls, Protocol issues for proxies, Security policy, Router as a security device, Router hardening

UNIT IV

Network Intrusion Detection: The roles of network IDS in a perimeter defence, IDS sensor placement, Virtual Private Networks: Advantages and Disadvantages of VPNs, IPSec basics, Other VPN, protocols PPTP & L2TP

UNIT V

Security protocols & Implementations: SSL/TLS, SSH, PGP, SHTTP, IPSec, Open SSL, Host hardening: Against local attacks, against network attacks, against application attacks, Antivirus solutions and deployment, Software updates and patches.

TEXT BOOKS:

1. 1. William Stallings(2017), Cryptography And Network Security: Principles and Practices, Seventh Edition, Pearson Publication.
2. 2. William Stallings, Lawrie Brown(2016), Computer Security: Principles and Practices, Second Edition, Pearson Publication.

Cloud and IoT Security

Prerequisite: NIL **Credit**: 3-3-5

Course Objectives:

1. To introduce the fundamental concepts of cloud computing, including its architecture, service and deployment models, and virtualization technologies.

2. To explore various cloud service platforms and assess their security challenges, including data and information security in the cloud.

3. To explain the architecture and design principles of IoT systems, with emphasis on frameworks, components, and communication models.

4. To examine wireless communication protocols and data management techniques relevant to IoT gateway devices.

5. To analyze web and message communication protocols for connected devices and evaluate privacy, security issues, and their mitigation in IoT systems.

Course Outcomes:

1. Describe the fundamental concepts of cloud computing and virtualization technologies including service models, deployment models, and virtualization layers. *(Understand)*

2. Analyze various cloud service platforms and evaluate security challenges related to data and information in cloud environments. *(Analyze/Evaluate)*

3. Explain the architecture, components, and design principles of IoT systems and their applications. *(Understand)*

4. Illustrate the use of wireless communication technologies and data management techniques at the IoT gateway level. *(Apply)*

5. Evaluate communication protocols and identify security vulnerabilities in IoT systems, suggesting appropriate solutions. *(Evaluate/Create)*

Course Structure:

UNIT I

Cloud Computing: Definition, roots of cloud computing, characteristics, cloud architecture, deployment models, service models.

Virtualization: Benefits & drawbacks of virtualization, server virtualization, virtualization of - operating system, platform, CPU, network, application, memory and I/O devices etc.

UNIT II

Cloud Computing Service Platforms, Compute services, storage services, database services, application services, queuing services, e-mail services, notification services, media services, content delivery services, analytics services, deployment & management services, identity & access management services and their case studies. Security in cloud computing: issues, threats, data security and information security.

UNIT III

Internet of Things (IoT): Overview, conceptual framework, architecture, major components, common applications Design principles for connected devices: Modified OSI Model for IoT/M2M systems, ETSI M2M Domains and High-level capabilities.

UNIT IV

Wireless communication technologies - NFC, RFID, Bluetooth BR/EDR and Bluetooth low energy, ZigBee, WiFi, RF transceiver and RF modules. Data enrichment, data consolidation & device management at gateway.

UNIT V

Design principles for web connectivity: web communication protocols for connected devices: constrained application protocol, CoAP Client web connectivity, client authentication, lightweight M2M communication protocol. Message communication protocols for connected devices - CoAP-SMS, CoAP-MQ, MQTT, XMPP. IoT privacy, security and vulnerabilities and their solutions.

TEXT BOOKS:

1. David Etter, " IoT Security: Practical guide book " Create Space, 1st Edition, 2016.
2. Drew Van Duren, Brian Russell, "Practical Internet of Things Security", Packt, 1st Edition, 2016.
3. Sean Smith, "The Internet of Risky Things", O'Reilly Media, 1st Edition, 2017.
4. Brian Russell, Drew Van Duren, "Practical Internet of Things Security: Design a security framework for an Internet connected ecosystem", 2nd Edition, 2018.

Ethical Hacking & Computer Forensics

Prerequisite: NIL   Credit : 3-3-5

Course Objectives

1. To introduce the principles and scope of Ethical Hacking, including hacker types, ethical responsibilities, and common attack vectors.

2. To provide foundational knowledge of scripting and programming skills, especially batch scripting, used in penetration testing and hacking tasks.

3. To develop hands-on skills in setting up secure and isolated environments, using virtualization tools for ethical hacking simulations.

4. To explain and explore key concepts and techniques in digital forensics, including forensic phases, file systems, and data recovery methods.

5. To familiarize students with industry-standard hacking and forensic tools, used for password cracking, packet sniffing, steganography, seizure, and analysis.

Course Outcomes:

1. Explain the fundamentals of Ethical Hacking, hacker classifications, and common attack techniques such as password cracking, email spoofing, DDoS, and steganography. *(Understand)*

2. Demonstrate the ability to write scripts and use batch programming for ethical hacking tasks. *(Create)*

3. Set up and configure a secure hacking environment using virtualization platforms and tools. *(Create)*

4. Explain the core concepts of digital forensics, including phases, file systems, and forensic investigation methods. *(Understand)*

5. Utilize various ethical hacking and digital forensic tools for analysis, simulation, and reporting. *(Apply/Create)*

Course Structure:

UNIT I

Introduction: Aims and Objectives, Technology involved and current issues in the IT industry, glimpse of information security, Ethical Hacking and Computer forensics.

UNIT II

Batch programming for Hacking. Penetration testing using NMAP, Metasploitable Linux: OS for penetration testing, Metasploit framework: Framework for exploiting.

UNIT III

Introduction to password cracking techniques. Exploring various password cracking tools: Cain & Abel, mimkatz, John the Ripper, RainbowCrack, etc. Various DoS attack techniques, DDoS attack and RDDoS attack.

UNIT IV

Introduction to Packet sniffing (WireShark, TCPDump, NetworkMiner, etc.), Keyloggers (keyghost/kidlogger, form grabbing), Email spoofing, DNS cache poisoning, Proxies/VPN (cyber ghost VPN), google dorks, Steganography (Invisible secrets, S tools), etc.

UNIT V

Introduction to computer forensics, cyber-crime, recent cyber-crimes within and outside the country. Phases of digital forensics to analyze cyber-crimes. Roles of law-enforcement and cyber-crime investigator in combating cyber-crimes

UNIT VI

Introduction to file systems. File structural details of how files get created and deleted at system level (for file systems: FAT, NTFS, Ext2/Ext3). Exploring computer forensic tools: TrueBack, CyberCheck, FTKImager, DFF (digital forensic framework), TSK (The sleuth Kit), Volatility framework, etc.

Text Books:

1. James S. Tiller, “The Ethical Hack: A Framework for Business Value Penetration Testing”, Auerbach Publications, CRC Press, 2004.
2. JOHN R. VACCA, Computer Forensics : Computer Crime Scene Investigation, Firewall Media.

Reference Books:

1. Kenneth C.Brancik “Insider Computer Fraud” Auerbach Publications Taylor & Francis Group -2008.
2. Bill Nelson, Amelia Phillips, Christopher Steuart, Guide to Computer Forensics and Investigations, 4e, Cengage Learning.

Cyber Crime, Cyber Laws & IPR

Prerequisite: NIL Credit : 3-0-3

Course Structure:

UNIT I

Information Technology & Cyber Crimes: Introduction, Glimpses, Definition and Scope, Nature and Extent, Know no Boundaries, Rapid Transmission and Accuracy, Diversity and Span of Victimization, Cyber World, Inadequacy of Law, Influence of Teenagers

Information Technology: Definition & Perspective, Growth & Future, Various Facets & Dimensions. **Regulatory Perspective on Technology:** Impact of Information and Technology, Regulation of CyberSpace, Legal Aspects of Regulation.

UNIT II

Technology & Forms of Cyber Crimes: Influence of Technology on Criminality, Forms of Cyber Crimes. **Computer Crimes & Cyber Crimes:** A Criminological Analysis Computer Crimes and Cyber Crimes: Terminological Aspects, Opportunities to Cyber Criminals, Motives of Offenders, Problems Affecting Prosecution, Cyber Crimes: Challenges of Prevention and Control.

UNIT III

Cyber Crimes 'and Global Response: Global Perspective, Country wise Legal Response, Country wise Analysis. Cyber Crimes and Indian Response: Introduction, The Indian Information Technology Act 2000, Preamble & Coverage, Nature of Offences and Penalties, Miscellaneous and Subsidiary Provisions Certain Shortcomings, Future Prospects and Needs.

UNIT IV

Mens Rea & Criminal Liability: Introduction, Historical Perspectives, Mens Rea in Indian Criminal Law, Mens Rea in English Criminal Law, Abetment of Offence, Criminal Liability and Role of Mens Rea in Indian Information Technology Act, 2000 Investigation in Cyber Crimes: Implications and Challenges: : Introduction, Procedural Aspects, Issues, Complications and Challenges Concerning Cyber Crimes, Problems and Precautionary measures for Investigation.

UNIT V

Cyber Crimes : Discovery and Appreciation of Evidences: Introduction, Law of Evidence, Evidence in Cyber Crimes : Challenges and Implications, Computer Generated Evidence and their Admissibility, Judicial Interpretation of Computer related Evidence

Prevention of Cyber Crimes :National and International Endeavours: Introduction, International Services on Discovery and Recovery of Electronic and Internet Evidence, International Organisation on Computer Evidence (IOCE), OECD Initiatives, Efforts of G-7 and G-8 Groups, Endeavours of Council of Europe, Measures of United Nations, Efforts of WTO, Measures of World Intellectual Property Organisation (WIPO),Interpol and its Measures, Efforts in India, Need of International Assistance and Appropriate Amendments, U.S. Laws on Cyber Crimes, U.S. Case-law on Cyber Evidences and Related Issues

TEXT BOOKS:

1. Dr Pramod Kr.Singh, “Laws on Cyber Crimes [Along with IT Act and Relevant Rules]” Book Enclave Jaipur India.

REFERENCE BOOKS:

1. Craig B, “Cyber Law: The Law of the Internet and Information Technology”. Pearson Education. Pawan Duggal, “Cyber Laws” Universal Law Publishing.

2. K.Kumar,” Cyber Laws: Intellectual property & E Commerce, Security”, First Edition, Dominant Publisher, 2011.

3. Rodney D. Ryder, “Guide to Cyber Laws”, Second Edition, Wadhwa And Company, New Delhi,

2007.

4. Vakul Sharma, "Handbook of Cyber Laws" Macmillan India Ltd, Second Edition, PHI, 2003.

5. Justice Yatindra Singh, "Cyber Laws", Universal Law Publishing, First Edition, New Delhi, 2003.

6. Sharma, S.R., “Dimensions of Cyber Crime”, Annual Publications Pvt. Ltd., First Edition, 2004.

7. Augastine, Paul T., “Cyber Crimes and Legal Issues”, Crecent Publishing Corporation, 2007.

Electives

Quantum Computing

Prerequisites: NIL **Credit:** 3-0-3

Course Objectives:

1. Understand fundamental concepts of quantum mechanics and information, including postulates of quantum theory, Dirac notation, and quantum circuit model.
2. Learn key quantum algorithms (Deutsch's, Bernstein-Vazirani, Grover's, Shor's) and protocols (teleportation, superdense coding) and apply them to solve problems in factoring and cryptography

Course Outcomes:

1. Understand the implications of quantum computing on cryptography.
2. Understand the foundations of post-quantum cryptography - Hack the RSA cryptosystem via a quantum computer.
3. Understand the quantum computing paradigm.
4. Understand the power and limitation of quantum computers.
5. State the four postulates of quantum mechanics and their application to computation.
6. Analyze fundamental quantum algorithms.

Detailed Syllabus

Brief history, the postulates of quantum theory, Dirac notation, and Quantum circuit model.

Qubit: The qubit state - matrix and Bloch sphere representation - computational basis – unitary evolution, Multi-qubit states - No-cloning theorem - Superdense coding - Pure states to Bell states – Bell inequalities.

Simple quantum protocols: teleportation, superdense coding, Deutsch's algorithm, Deutsch-Jozsa Algorithm and the Bernstein-Vazirani Algorithm.

Introduction to Factoring and RSA cryptosystem. Factoring and Period Finding. Quantum Fourier Transform. Shor's Algorithm.
Grover's search algorithm, Applications of Grover's Search Algorithm.

Reference books:

1. Nielsen, Michael A., and Isaac L. Chuang. Quantum Computation and Quantum Information. Cam-
bridge, UK: Cambridge University Press, September 2000.
2. Lecture notes by Prof. John Preskill, California Institute of Technology.

Post Quantum Cryptography

Detailed Syllabus

Introduction to Cryptography - Symmetric Key Encryption – AES Block Cipher, Public Key Encryption – RSA Encryption scheme, El Gamal Encryption scheme. Key Encapsulation Scheme. Digital Signature Scheme – RSA Signature scheme, Schnorr Signature scheme.

Quantum Algorithms: Shor's algorithm, Grover's algorithm. Impact of quantum computing on currently deployed cryptosystems: Impact on factoring problem, Discrete Logarithm problem. Impact on Symmetric key cryptosystem and collision finding in hash function.

Lattice-based Post-Quantum Cryptosystems: Basics of lattice-based cryptography: NewHope, Kyber and Saber (NIST post-quantum candidates). Classical constructions - NTRU, NTRU Prime. Digital Signa- ture Algorithm: Dilithium, Falcon.

Code-based Post-Quantum Cryptosystems: Basics of Code-based cryptography, Classic McEliece encap- sulation scheme, Hamming Quasi-Cyclic (HQC) encapsulation scheme.

Multivariate-based Post-Quantum Cryptosystems: Basics of Multivariate-based cryptography. Unbalanced oil and vinegar scheme, Rainbow signature scheme, Hidden Field Equations scheme.

Isogeny-based Post-Quantum Cryptosystems: Basics of Isogeny based cryptography, Supersingular Isogeny based Key Exchange (SIKE), Digital Signature Algorithm based on Isogeny.

Reference books:

1. Daniel J. Bernstein, Johannes Buchmann and Erik Dahmen, "Post-Quantum Cryptography", Springer, 2009.
2. Relevant research articles

Others:

1. https://csrc.nist.gov/projects/post-quantum-cryptography
2. https://pqcrypto.org/index.html

Cloud Computing

Prerequisite: Nil
Course outcomes:

CO1	Articulate the main concepts, key technologies, strengths, and limitations of cloud computing and the possible applications for state-of-the-art cloud computing
CO2	Identify the architecture and infrastructure of cloud computing, including SaaS, PaaS, IaaS, public cloud, private cloud, hybrid cloud, etc.
CO3	Choose a suitable technique to address security, interoperability issues
CO4	Provide the appropriate cloud computing solutions and recommendations according to the applications used

Syllabus:

Introduction to Cloud Computing, Gartner's Hype Cycle for Emerging Technologies, Comparisons: Cluster, Grid and Cloud, Cloud Computing at a Glance, Vision, A Close Look, The NIST Model, Cloud Cube Model, Types: Deployment and Service Models, Public, Private, Hybrid and Community Cloud, IaaS, PaaS, SaaS, Characteristics, Applications, Benefits, Disadvantages, Web 2.0, The Laws of Cloudonomics, Obstacles, Cloud Adoption, Measuring the Costs, Service-Level Agreement, Cloud Architecture, Virtual Appliances, Connecting to the Cloud, IaaS Workloads, Open SaaS and SOA, On Demand vs. On Premises IT, Bird's-Eye View of Cloud Computing Vendors, Virtualization, Characteristics of Virtualized Environments, Taxonomy of Virtualized Techniques, Full Virtualization, Paravirtualization, Partial Virtualization, Pros and Cons of Virtualization, Hypervisor

Cloud issues and challenges - Properties - Characteristics - Service models, Deployment models Virtualization – Virtual Machines, Resource Allocation, Leases: Advance Reservation, Best Effort, Immediate, Deadline Sensitive and Negotiated, Swapping and Backfilling, Resource Allocation Measures, Task Scheduling, Task: Dependent and Independent, Job, Application, Workflow: Montage, Epigenomics, SIPHT, LIGO, CyberShake, Machine: Homogeneous and Heterogeneous, Mode: Immediate, Intermediate and Batch, Expected Time to Compute Matrix, Manager Server, Data Center, Virtual Machine, Server, Makespan, Resource Utilization, Average Execution Time, Uncertainty

Introduction to Energy Efficient Task Consolidation, Energy-Conscious Task Consolidation, MaxUtil, Energy-Aware Task Consolidation, Virtual Cluster, CPU Utilization Threshold, Sleep or Power Saving Mode, High-Throughput Computing: Task Computing and Task-based Application Models, Market-Based Management of Clouds, Green Cloud Computing Architecture, Federated Clouds, Pricing Mechanism, SLA Violation.

Introduction to Cloud Security, Case Studies: Manjrasoft Aneka, Amazon Web Services, Google Cloud Platform, Microsoft Azure, Programming support of Google App Engine, Virtual Machine and its Provisioning, Time and Space-shared Provisioning.

References:

Textbooks:

1. R. Buyya, C. Vecchiola and S. T. Selvi, Mastering Cloud Computing Foundations and Applications Programming, Morgan Kaufmann, Elsevier, 2013.

2. B. Sosinsky, Cloud Computing Bible, Wiley, 2011.

Reference books:

3. D. N. Chorafas, Cloud Computing Strategies, CRC Press, Taylor and Francis Group, 2011.

4. Kai Hwang, Geoffrey C. Fox and Jack J. Dongarra, “Distributed and cloud computing from Parallel Processing to the Internet of Things”, Morgan Kaufmann, Elsevier , 2012.

5. D. Janakiram, Grid Computing, Tata McGraw-Hill, 2005.

Data Privacy

Prerequisites: Nil **Credit**: 3-0-3

Course Objectives:

1. Understand the principles, significance, and legal frameworks of data privacy in modern computing systems.
2. Analyze various privacy threats, attack models, and formal privacy-preserving models.
3. Explore core techniques such as anonymization, differential privacy, and cryptographic approaches for protecting data.
4. Apply privacy-preserving methods in practical settings, including data publishing and machine learning applications.
5. Gain hands-on experience with tools and frameworks that implement privacy-preserving technologies.

Course Outcomes:

1. Explain the importance of data privacy and interpret legal, ethical, and regulatory frameworks governing data usage.
2. Analyze privacy threats and apply formal models such as k-anonymity, l-diversity, t-closeness, and differential privacy to safeguard sensitive data.
3. Evaluate and implement data anonymization and perturbation techniques including masking, generalization, and synthetic data generation.
4. Apply cryptographic methods such as Secure Multi-party Computation, Homomorphic Encryption, and Private Set Intersection to enable privacy-preserving computations.
5. Assess privacy vulnerabilities in machine learning systems and apply mitigation strategies like federated learning and differentially private training algorithms.

Detailed Syllabus

Introduction to Data Privacy: Importance of data privacy in the digital age, Case studies: Privacy breaches and consequences, Legal and regulatory landscape: GDPR, HIPAA, Indian IT Act. Definitions: Privacy vs. Security vs. Confidentiality

Privacy Models and Attacks: Adversarial models, Linkage attacks and re-identification, k-anonymity, l-diversity, t-closeness, Limitations of syntactic anonymization.

Differential Privacy: Formal definition and intuition, Mechanisms: Laplace, Gaussian, Composition theorems, Local differential privacy, Applications: Census, machine learning.

Privacy-Preserving Data Publishing: Data masking and generalization, Data perturbation and noise addition, Synthetic data generation, Randomized response.

Cryptographic Approaches: Secure Multi-party Computation (SMPC), Homomorphic Encryption, Private Set Intersection (PSI), Zero-Knowledge Proofs (overview).

Privacy in Machine Learning: Federated learning and privacy, Membership inference attacks, Differentially private stochastic gradient descent (DP-SGD), Model inversion and mitigation techniques.

References:

1. Solove, Daniel J. *Understanding Privacy*, Harvard University Press, 2008.
2. **Sweeney, L.** *k-Anonymity: A Model for Protecting Privacy*, International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems, 2002.
3. **Dwork, C., & Roth, A.** *The Algorithmic Foundations of Differential Privacy*, Foundations and Trends in Theoretical Computer Science, 2014.
4. **Lindell, Y.** *Secure Multiparty Computation for Privacy-Preserving Data Analysis*, CACM, 2020.

Intelligent Systems

Module 1

Introduction to agents – Structure of intelligent agents, Problem solving agents – Formulating problems – Overview of uninformed searching strategies, informed search methods, Game playing as search.

Module 2

Knowledge based agent representation – Logics – First Order logic – Reflex agents – Building a knowledge base – General ontology – Inference – Logical recovery. Planning agents – Planning in situational calculus – Representation of Planning – Partial order Planning – Practical Planners – Conditional Planning.

Module 3

Agents acting under uncertainty – probability notation – Bayes rule, Probabilistic reasoning – Belief networks – Utility theory – Decision network – Value of information learning agents – Learning from Observations – Knowledge in Learning, Case studies on applications of AI.

References

Books

- Russell S and Norvig P, "Artificial Intelligence – A modern approach", Third Edition, Prentice Hall, 2009.

Resources

- Elaine Rich, Kevin Knight and Shivashankar B. Nair, "Artificial Intelligence", Third Edition, TMH Educations Private Limited, 2008
- Nilsson N J, "The Quest for Artificial Intelligence", Cambridge University Press, 2009.

Unmanned Aerial Vehicle

Credit:3-0-3

Prerequisite	Flight Mechanics, Classical Control Theory
Course Objectives	1. To understand the working principles and importance of unmanned aerial vehicles (UAV) in various sectors. 2. To comprehend the design and construction of different types of UAVs. 3. To understand the use of UAVs in military and civilian applications. 4. To analyze the operational status of UAVs.
Course Outcomes	1. Understand the principles of UAV design and construction. 2. Gain knowledge about the different applications of UAVs. 3. Demonstrate an understanding of the working principles of UAVs. 4. Select the most suitable UAV for a specific application.

Detailed Syllabus

Definition and history of UAVs Types of UAVs (fixed-wing, rotary-wing, hybrid), UAV components (airframe, propulsion system, guidance and control, payload), UAV Flight Dynamics, Basic principles of flight, Flight performance, Stability and control of UAVs, Flight control systems.

Types of sensors (optical, infrared, radar, etc.), Payload selection and integration Data acquisition and processing, UAV navigation: accelerometers, gyros, GPS. Path planning algorithms: Dubin's curves, way-points, Voronoi partitions. Path following and guidance: Straight line and curve following, vision based guidance.

Future directions and the road ahead, Radio communication principles, Communication protocols and frequencies, Ground control stations, Regulations governing UAVs, Safety and ethical considerations, Privacy and security concerns.

Civilian and military applications of UAVs, Agricultural, environmental, and disaster management applications, UAVs for surveillance and reconnaissance

Reference books:

1. Randal W. Beard and Timothy W. McLain: Small Unmanned Aircraft:
2. Theory and Practice, Princeton University Press, 2012
3. Kimon P. Valavanis: Advances in Unmanned Aerial Vehicles: State of the Art and the Road to Autonomy, Springer, 2007

Machine Learning

Prerequisite	Probability and Statistics, Basics in programming
Course Objectives	1. To familiarize the students with traditional and modern learning paradigms with their applications in the real-world systems 2. To instill adaptation of human training for development of intelligent machines 3. To inculcate modeling of a real-world practical problem in a machine learning domain 4. To introduce modern artificial neural networks and to develop an understanding of the deep learning techniques 5. To explore some open areas of research and explore directions for their possible solutions
Course Outcomes	After completion of this course the students will be able to: 1. Model a real-world problem in the machine learning domain. 2. Use information, patterns and past results in training a machine learning model. 3. Use knowledge of predictability in business decision making. 4. Enhance deep learning skills for problem solving where hard-computation the based approach fails. 5. Develop sub-optimal or heuristic solutions to computationally hard problems.

Detailed Syllabus

Introduction to machine learning: learning systems, classification, clustering, regression, separability of problems; introduction to learning paradigms: supervised, unsupervised, semi-supervised, active, reinforcement with examples; cross-validation; performance evaluation metrics for classification and clustering; curse of dimensionality, feature selection, reduction and expansion, computation of Eigen coordinates and principal component analysis.

Recognition systems and design cycle, Non-linearly separable problems: solutions through Cover's theorem with examples, parametric learning mechanisms like Maximum likelihood, expectation maximisation, aposteriori probabilities, Instance-based learning, Lazy learning with K-nearest neighbour, Eager learning with basis functions, non-parametric learning using support vector machines (SVMs). Artificial neural networks: Analogy of biological neural network with artificial neural network; Perceptron learning; gradient descent algorithm; multi-layer perceptrons; back-propagation algorithm; activation functions, delta rule, learning curves: overfitting and underfitting of models; Hebbian learning, self organising feature map, radial basis function neural networks.

Deep neural networks: Introduction and advent of deep learning paradigm, solutions to vanishing and exploding gradient problems, regularisation, activation functions for deep learning, deep feed forward network, convolutional neural network (CNN), pre-trained CNN models. Attention network, generative models like auto-encoders and adversarial learning, recurrent neural networks, problem solving through deep learning and open areas of research and applications.

Text books:

1. T. M. Mitchell, Machine Learning, McGraw-Hill, 1997.
2. S. Haykin, Neural Networks: A Comprehensive Foundation. Prentice-Hall of India, 2007.

Reference books:

1. R. O. Duda, P.E. Hart, D. G. Stork, Pattern Classification, John Wiley, 2001.
2. I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning, MIT Press, 2016.

Natural Language Processing

Credit:3-0-3

Prerequisite	Nil
Course Objectives	1. Understand approaches to syntax and semantics in NLP. 2. Understand approaches to discourse, generation, dialogue and summarization within NLP. 3. Understand current methods for statistical approaches to machine translation. 4. Understand machine learning techniques used in NLP, including hidden Markov models and probabilistic context-free grammars, clustering and unsupervised methods, log-linear and discriminative models, and the EM algorithm as applied within NLP.
Course Outcomes	1. Identify the different linguistic components of natural language. 2. Evaluate a morphological analyser for a given natural language. 3. Apply appropriate parsing techniques necessary for a given language. 4. Design a new tagset and a tagger for a given natural language. 5. Develop applications involving natural language.

Detailed Syllabus

Morphology And Part-Of-Speech Processing: Introduction –Regular Expressions and Automata-Non- Deterministic FSAs. Transducers –English Morphology-Finite-State Morphological Parsing -Porter Stemmer -Tokenization-Detection and Correction of Spelling Errors. N-grams –Perplexity -Smoothing-Interpolation -Backoff . Part-of-Speech Tagging –English Word Classes -Tagsets -Rule-Based -HMM-Transformation-Based Tagging -Evaluation and Error Analysis. Hidden Markov and Maximum Entropy Models Speech Processing: Phonetics –Articulatory Phonetics -Phonological Categories -Acoustic Phonetics and Signals -Speech Synthesis–Text Normalization –Phonetic and Acoustic Analysis -Diphone Waveform synthesis –Evaluation-Automatic Speech Recognition – Architecture -Hidden Markov Model to Speech -MFCC vectors -Acoustic Likelihood Computation -Evaluation. Triphones –Discriminative Training -Modeling Variation. Computational Phonology- Finite-State Phonology –Computational Optimality Theory - Syllabification -Learning Phonology and Morphology. Syntax Analysis: Finite- State and Context-Free Grammars -Dependency Grammars. Syntactic Parsing – Ambiguity -Dynamic Programming Parsing Methods –CKY-Earley and Chart Parsing-Partial Parsing-Evaluation. Statistical Parsing – Probabilistic ContextFree Grammars –Probabilistic CKY Parsing of PCFGs –Probabilistic Lexicalized CFGs – Collins Parser – Shallow parsers – Dependency parsing. Semantic and Pragmatic Interpretation: Representation of Meaning –Desirable Properties -Computational Semantics -Word Senses -Relations Between Senses –WordNet -Event Participants-Proposition Bank -Frame Net -–Metaphor. Computational Lexical Semantics –Word Sense Disambiguation-Supervised Word Sense Disambiguation- Dictionary and Thesaurus Methods-Word Similarity -Minimally Supervised WSD - Hyponymy and Other Word Relations -Semantic Role Labeling -Unsupervised Sense Disambiguation. Computational Discourse -Discourse Segmentation - Unsupervised Discourse -Segmentation -Text Coherence -Reference

Resolution –Phenomena –Features and algorithms -Pronominal Anaphora Resolution. Applications: Information Extraction –Named Entity Recognition -Relation Detection and Classification –Temporal and Event Processing -Template-Filling -Biomedical Information Extraction. Question Answering and Summarization - Information Retrieval -Factoid Question Answering -Summarization -Single and Multi-Document Summarization - Focused Summarization -Evaluation. Dialog and Conversational Agents –Properties of Human Conversations -Basic Dialogue Systems

Text books:

1. Jurafsky and Martin, “Speech and Language Processing”, Pearson Prentice Hall, Second Edition, 2008.
2. Christopher D. Manning and Hinrich Schütze, “Foundations of Statistical Natural Language Processing”, MIT Press, 1999.

Reference books:

1. Stevan Bird, “Natural Language Processing with Python”, Shroff, 2009.
2. James Allen, “Natural Language Understanding”, Addison Wesley, Second Edition, 2007.

Information Retrieval

Credit:3-0-3

Prerequisite	Nil
Course Objectives	1. To introduce the fundamental concepts and trends in information retrieval systems. 2. To familiarize students with the different types of information retrieval systems and their components 3. To empower students to evaluate and select appropriate information retrieval techniques. 4. To instill knowledge of Information retrieval as a research field, its challenges and future research directions. 5. To assess different search models and their basic structure.
Course Outcomes	Students will be able to: 1. To present the basic concepts in information retrieval and more advance techniques of multi-modal based information systems 2. To understand the underlined problems related to information retrieval. 3. To acquire the necessary experience to design and implement real applications using information retrieval systems 4. Analyze evaluation and performance of retrieval techniques.

Detailed Syllabus

Introduction to Information Retrieval: The nature of unstructured and semi-structured text. Inverted index and Boolean queries. Text Indexing, Storage and Compression, Text encoding: tokenization, stemming, stop words, phrases, index optimization. Index compression: lexicon compression and postings lists compression. Gap encoding, gamma codes, Zipf's Law. Index construction. Postings size estimation, merge sort, dynamic indexing, positional indexes, n-gram indexes, real-world issues.

Retrieval Models: Boolean, vector space, TFIDF, Okapi, probabilistic, language modeling, latent semantic indexing. Vector space scoring. The cosine measure. Efficiency considerations. Document length normalization. Relevance feedback and query expansion. Rocchio, Performance Evaluation: Evaluating search engines. User happiness, precision, recall, F-measure. Creating test collections: kappa measure, interjudge agreement.

Text Categorization and Filtering: Introduction to text classification. Naive Bayes models. Spam filtering. Vector space classification using hyperplanes; centroids; k Nearest Neighbors. Support vector machine classifiers. Kernel functions. Boosting, Text Clustering: Clustering versus classification.

Partitioning methods. k-means clustering. Mixture of gaussians model. Hierarchical agglomerative clustering. Clustering terms using documents.

Advanced Topics: Summarization, Topic detection and tracking, Personalization, Question answering, Cross language information retrieval, Web Information Retrieval: Hypertext, web crawling, search engines, ranking, link analysis, PageRank, HITS. Retrieving Structured Documents: XML retrieval, semantic web.

Reference books:

1. Introduction to Information Retrieval Manning, Raghavan and Schutze, Cambridge University Press.
2. Modern Information Retrieval Baeza-Yates and Ribeiro-Neto, Addison Wesley, 1999.
3. A comprehensive survey by Ed Greengrass Mining the Web, Soumen Charabarti, Morgan-Kaufmann, 2002.

Artificial Intelligence

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

CO1	Solve searching problems using A*, Mini-Max algorithms.
CO2	Create logical agents to do inference using first order logic.
CO3	Understand Bayesian Networks to do probabilistic reasoning..
CO4	Perform Statistical learning using EM algorithm

Syllabus:

Formalized symbolic logic: Propositional logic-first order predicate logic, wff conversion to clausal form, inference rules, the resolution principle, Dealing with inconsistencies and uncertainties, fuzzy logic.

Probabilistic Reasoning Structured knowledge, graphs, frames and related structures, Knowledge organization and manipulation.

Matching Techniques, Knowledge organizations, Management.

Natural Language processing, Pattern recognition, expert systems.

Text Book(s):

Artificial Intelligence, Dan W Patterson, Prentice Hall of India.
Artificial Intelligence, Nils J. Nilsson, Elsevier

References & Web Resources:

E. Rich and K. Knight, Artificial Intelligence, TMH.
Stuart Russell, Peter Norvig, Artificial Intelligence - A Modern Approach, 3/e, Pearson, 2003.

Machine Learning Applications for Cyber Security

Course Objectives

- An overview of different AI and Machine Learning models in Cyber Security
- Using Machine Learning for effective security
- Various attack on ML models
- Machine Learning and Privacy

Course Outcome

- Understand the concepts in Machine Learning
- Learn various AI and Machine learning models for cyber security
- Ability to apply AI and machine learning models in cyber security issues

Course Structure:
Introduction: Role of AI in Cyber Security and Security Framework: Artificial Intelligence in Cyber Security, Challenges and Promises, Security Threats of Artificial Intelligence,

Use-Cases: Artificial Intelligence Email Observing, Programming in Python and Basics of manipulation of Data. Machine Learning in Security: Introduction to Machine Learning,

Applications of Machine Learning in Cyber Security Domain, Machine Learning: tasks and Approaches, Anomaly Detection, Privacy Preserving

Nearest Neighbour Search, Machine Learning Applied to Intrusion Detection, Online Learning Methods for Detecting Malicious Executables Deep Learning in Security: Introduction to deep learning,

Cyber Security Mechanisms Using Deep Learning Algorithms, Applying deep learning in various use cases, Network Cyber threat Detection Artificial Intelligence in Cyber Security: Model Stealing & Watermarking, Network Traffic Analysis, Malware Analysis

Reference Books

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

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

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

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

5. Machine Learning: A Probabilistic Perspective, Kevin P Murphy, MIT Press.

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

Secure Machine Learning

Course Objectives

1. To provide foundational understanding of machine learning (ML) techniques and their application in security contexts.
2. To study common vulnerabilities in ML systems and adversarial attack vectors.
3. To explore secure learning algorithms that are robust to evasion and poisoning attacks.
4. To understand privacy-preserving techniques such as differential privacy and federated learning.
5. To design secure, ethical, and trustworthy ML-based systems for real-world applications.

Course Outcomes (COs)

After successful completion of the course, students will be able to:

1. Explain the security challenges and vulnerabilities in ML systems. (Understand)
2. Analyze and evaluate various adversarial attacks and defenses on ML models. (Analyze/Evaluate)
3. Apply robust learning techniques to design ML models resilient to security threats. (Apply/Create)
4. Implement privacy-preserving ML techniques such as differential privacy and federated learning. (Apply)
5. Critically assess the ethical, fairness, and deployment considerations of secure ML systems. (Evaluate)

Unit I: Introduction to Machine Learning and Security

Overview of machine learning: supervised, unsupervised, reinforcement learning, ML lifecycle and security implications, ML in cybersecurity: malware detection, fraud detection, anomaly detection, Threat models for ML systems: black-box, white-box, and gray-box, Introduction to attack surfaces in ML systems

Unit II: Adversarial Attacks on Machine Learning Models

Adversarial examples in classification, Evasion attacks on neural networks (FGSM, PGD, CW attack), Poisoning attacks: label flipping, backdoor injection,Model inversion and membership inference attacks, Security implications in real-world ML deployments

Unit III: Defenses and Robust ML Techniques

Adversarial training, Defensive distillation, Certified robustness techniques, Gradient masking and its pitfalls, Robust optimization and regularization strategies

Unit IV: Privacy-Preserving Machine Learning

Data privacy vs model privacy, Differential privacy: concepts and implementation, Secure multiparty computation (SMC), Homomorphic encryption in ML, Federated learning and its security/privacy challenges

Unit V: Trustworthy, Fair, and Ethical ML

Explainability and interpretability in secure ML, Fairness and bias in ML models, Accountability and auditability, Ethics in AI/ML system design, Case studies: Security-sensitive ML applications (healthcare, finance, surveillance)

Textbooks

1. "Adversarial Machine Learning" by Anthony D. Joseph, Battista Biggio, and Blaine Nelson – Springer
2. "Machine Learning and Security" by Clarence Chio and David Freeman – O'Reilly Media
3. "Security and Privacy in Machine Learning" by Reza Shokri and Vitaly Shmatikov (Lecture Notes, available online)
   Reference Books and Resources
1. Ian Goodfellow, Yoshua Bengio, and Aaron Courville – Deep Learning, MIT Press
2. Nicolas Papernot et al. – Research papers on adversarial ML (available via arXiv.org)
3. NIST Special Publication 1270 – Towards a Standard for AI Security and Trustworthiness
4. Open-source toolkits: CleverHans, IBM Adversarial Robustness Toolbox (ART), TensorFlow Privacy