INDIRA GANDHI DELHI TECHNICAL UNIVERSITY FOR WOMEN
(Established by Govt. of Delhi vide Act 9 of 2012)

M.Tech.- IT (Cyber Security)

First Semester

S. No.	Code	Subject	L-T-P	Credits	Category
1.	MIS-101	Advanced Programming	3-0-2	4	DCC
2.	MIS-103	Advances in Machine Learning	3-0-2	4	DCC
3.	MCS-105	Advanced Data Structures and Algorithms	3-0-2	4	DCC
4.	MIS-105	Fundamentals of Information Security	3-1-0	4	DCC
5	GEC-101	Generic Open Elective – I	2-0-0 1-1-0 0-0-4	2	GEC
6.	DEC-1xx	Departmental Elective Course - 1	3-1-0/ 3-0-2	4	DEC
		Total Credits		**22**	

Second Semester

S. No.	Code	Subject	L-T-P	Credits	Category
1.	MIS-102	Secure Coding and Security Engineering	3-0-2	4	DCC
2.	MIS-104	Applied Cryptography	3-0-2	4	DCC
3.	DEC-1xx	Departmental Elective Course – 2	3-0-2/ 3-1-0	4	DEC
4.	DEC-1xx	Departmental Elective Course – 3	3-0-2/ 3-1-0	4	DEC
5.	DEC-1xx	Departmental Elective Course – 4	3-0-2/ 3-1-0	4	DEC
6	ROC-902	Research Methodology and Publication Ethics	3-1-0	4	ROC
		Total credits		**24**	

Third Semester

Track-1

S. No.	Code	Subject	L-T-P	Credits	Category
1.	DEC-2xx	Departmental Elective-5	3-0-0/ 2-0-2	3	DEC
2.	DEC-2xx	Departmental Elective-6	3-0-0/ 2-0-2	3	DEC
3.	GEC-201	General Open Elective - II	2-0-0 1-1-0 0-0-4	2	GEC
4.	MIS-251	Dissertation – I	-	6	ROC
5.	MIS-253	Summer Industrial Training/Internship	-	1	ROC
		Total credits		**15**	

Track-2 Research Project

S.N.	Code	Subject	L-T-P	Credits	Category
		Generic Open Elective-II	2-0-0/ 1-1-0/ 0-0-4	2	GEC
		Research Project Work-I		12	ROC
		Summer Industrial Training/Internship		1	ROC
Total Credits				**15**	

Track -3 Industry Project

S.N.	Code	Subject	L-T-P	Credits	Category
		Generic Open Elective-II	2-0-0/ 1-1-0/ 0-0-4	2	GEC
		Industry Project Work-I		12	ROC
		Summer Industrial Training/Internship		1	ROC
Total Credits				**15**	

Fourth Semester

S. No.	Code	Subject	L-T-P	Credits	Category

1.	MIS-252	Dissertation – II/Project Work-II/Research Project Work-II	-	20	ROC
		Total credits		**20**	

List of Departmental Elective Courses

Category	**Course Code**	**Subject**	**Credits**
Departmental Elective Course-1	MIS-107 MIS-109 MIS-111	Cyber Security and Forensics Digital Identity and Access Management Cyber Threat Intelligence	3-0-2 3-0-2 3-1-0
Departmental Elective Course-2	MIS-106 MIS-108 MIS-110	Mathematics for Machine Learning Cyber Risk Management Cryptographic Protocols and Algorithms	3-1-0 3-1-0 3-1-0
Departmental Elective Course-3	MIS-112 MIS-114 MIS-116	Security Patterns Applications of Machine Learning in Cyber Security Advanced Network Technology	3-0-2 3-0-2 3-0-2
Departmental Elective Course-4	MIS-118 MIS-120 MIS-122	Cyber Laws and Rights Security and Privacy in Social Networks Software Defined Networks	3-1-0 3-1-0 3-1-0
Departmental Elective Course-5	MIS-201 MIS-203 MIS-205	Ethical Hacking Cloud Computing Architecture and Security Security Testing and Risk Management	3-0-0 2-0-2 2-0-2
Departmental Elective Course-6	MIS-207 MIS-209 MIS-211	Natural Language Processing Neural Networks and Deep Learning Blockchain Fundamentals	2-0-2 2-0-2 2-0-2

Secure Coding and Security Engineering	
Course Code: MIS-102 Contact Hours: L-3 T-0 P-2 Course Category: DCC	Credits : 4 Semester: 2

Introduction: Security breaches in software are costing companies large fines and regulatory burdens. Developing software, that is reliable in its functionality, resilient against attackers, and recoverable when the expected business operations are disrupted, is a must have. The assurance of confidentiality, integrity and availability is becoming an integral part of software development. This course is being introduced to integrate security principles and secure programming with Software development to reduce effort in removing basic vulnerabilities and risk thereby. The course is effective in enabling students to learn and develop software that is reliable and resilient to software attacks.

Course Objective

- To learn Secure Software Development Guidelines and Best Practices.
- To learn secure programming practices so as to build secure software resilient to cyber attacks.
- To learn secure configuration of various tiers and layers involved in Software Development.

Pre-requisite:

- Basic Knowledge of Programming Language (s), Database Management, Network, Server

Course Outcome: Upon successful completion of this course, students will be able to:

- Acquire security requirements with respect to software development.
- Design and implement software development with minimum software vulnerabilities.
- Write and test software code with respect to security testing and remove security flaws.

Pedagogy

Lectures will be imparted along with hands on lab sessions and latest real world case studies about software vulnerabilities reported, prevention and patching techniques.

Contents

UNIT-I	**10 Hours**
Secure software development life-cycle: Software development life cycle (Microsoft, McAfee, OWASP etc), development team, Quality and Security, Application Guidelines, (ISC)^2 Ten best practices of secure software development, Security principles, Security Standards Three pillars of software security, Seven Touch points of software security, Security Methodologies, Security Framework, Security Models	
UNIT-II	**10 Hours**
Secure Software Requirements: Introduction, Objective, Sources, Types of Security Requirements, Requirements Engineering for Secure Software, Concepts of Misuse and Abuse, SQUARE Process Model, SQUARE Sample Outputs, Requirements Elicitation and Prioritization, Object Modeling, Threat Modeling Secure Software Design: Design Consideration, processes, Architecture, technologies,	

UNIT-III	**12 Hours**
Secure Software Implementation, : Introduction to Software Vulnerability and Preventive/ Defensive techniques , Vulnerability description, types, Vulnerability Databases, OWASP top 10, NVD, CWE, Common Software Vulnerabilities and Controls, Defensive Coding Practices—Concepts and Techniques : Buffer Overrun, Format String Problems, Integer Overflow, and Injection flaws : SQL Injection, Command	
Injection, Failure to Handle Errors, Cross Site Scripting, Broken Authentication and Session Management, Magic URLs, Weak Passwords, Failing to Protect Data, Weak random numbers, improper use of cryptography, Insecure Direct Object References, Insecure De-serialization, Security Mis-configuration, Information Leakage, Race Conditions, Poor Usability, Not Updating Easily, Executing with too much privilege, Failing to protect network traffic, improper use of PKI, trusting network name resolution	
UNIT-IV	**10 Hours**
Secure Coding Standards: Memory Management, Exception management, Development tools, IDEs tools, Versioning tools, Networking tools, Coding in the cube: Functions, procedures and code blocks, Structuring for Validation, Structured Programming, Debugging, Coding and applying security requirements during maintenance, Security code analysis and review: Code review with a tool (fortify, coverty etc), Code analysis Securing Server, Database, Network and their secure configuration, Firewalls, Case Study : Recent Software vulnerabilities due to insecure programming and how to prevent them during design and implementation	
Text Books	
1	Paul, M. (2016). Official (ISC) 2 Guide to the CSSLP. CRC Press.
2	SEACORD, R. (2013). Secure Coding in C and C++ (2nd Edition). SEI Series in Software Engineering
3	Howard, Michael, David LeBlanc, and John Viega. "24 Deadly Sins of Software Security." Programming Flaws and How to Fix Them (2010). McGraw-Hill Education
Reference Books	
1	Ransome, J., & Misra, A. (2018). Core software security: Security at the source. CRC press.
2	Bishop, M. (2019). Computer Security(2nd Edition). Addison-Wesley Professional.
3	McGraw, G. (2006). Software security: building security in (Vol. 1). Addison-Wesley Professional
4	John Veiga, Gary Mc Graw, "Building Secure Software: How to Avoid Security Problems the Right Way", Addison-Wesley Professional Computing Series, 2001

APPLIED CRYPTOGRAPHY	
Course Code: MIS-104 Contact Hours: L-3 T-0 P-2 Course Category: DCC	Credits: 4 Semester: 2

Introduction:

This course will introduce students to the basic building blocks of cryptography and applications of cryptographic protocols in real world. The focus will be on how cryptography and its application can maintain privacy and security in electronic communications and computer networks.

Course Objectives:

- To understand the fundamentals of Cryptography
- To acquire knowledge on standard algorithms used to provide confidentiality, integrity and authenticity

Pre-requisite: None

Course Outcome: Upon successful completion of this course, students will be able:

- To explain and use modern cryptographic methods (symmetric encryption, public key encryption, hash functions, key management, digital signatures, certificates)
- To implement and identify electronic mail security system, SSL/TLS and recent developments affecting security and privacy on the Internet.
- To apply and use cryptographic concepts to real world problems

Pedagogy: Emphasis on lab sessions where students will be given programming assignments to code in lab based on topics learnt in previous lectures.

Contents

UNIT-I	10 Hours
Course Introduction and terminology, Conventional Cryptography: Definitions, Classical encryption techniques, One time pad, Perfect Secrecy, DES, Triple DES, Finite fields, AES, Modes of Encryption	
UNIT-II	11 Hours
Asymmetric Cryptography: Number Theory, public key cryptography: RSA, ElGamal, and Elliptic Curve Cryptography, Diffie Hellman Key management , Digital Certificates: X.509	
UNIT-III	11 Hours
Stream Ciphers, LFSR based stream ciphers, Message Authentication Codes, Hash functions, Hash algorithms, Digital Signatures and Authentication Protocols, Firewalls	
UNIT-IV	10 Hours
Intrusion Detection, PGP, S/MIME, Kerberos, IPSec, SSL/TLS, Password Hashing and Management	
Text Books	
1	W Stallings, “Cryptography and Network Security: Principles and Practice, 6/e”, Prentice Hall

2	B. Forouzan, D. Mukhopadhyay, "Cryptography and Network Security 2/e", Tata-McGraw Hill
3	Christof Paar, Jan Pelzl, “Understanding Cryptography: A textbook for students and practitioners, 1/e”, Springer
4	Bernard Menezes, “Network Security and Cryptography 2/e”, Cenege Learning
Reference Books	
1	A. Menezes, P. van Oorschot, S. Vanstone. “Handbook of Applied Cryptography”, CRC press, 1997.
2	Douglas R. Stinson, “Cryptography: Theory and Practice 3/e”, CRC Press, 2006
3	B. Schneier. “Applied Cryptography”. Second Edition. John Wiley & Sons, Inc., 1996

MATHEMATICS FOR MACHINE LEARNING	
Course Code: MIS 106 Contact Hours: L-3 T-1 P-0 Course Category: DEC	Credits: 4 Semester: 2

Introduction: This course introduces basic mathematical concepts related to Machine learning

Course Objective:

- To understand basic concepts of Linear Algebra
- To introduce some fundamental concepts about Matrices and Matrix decomposition.
- To provide the concepts of Probability and Distributions
- To understand concepts of Vector Calculus and Gradients

Pre-requisite: Nil

Course Outcome: After studying this course, students will be able to:

- Develop new algorithms for Machine learning.
- Solve Classification Problems using Matrix Decomposition and Optimization concepts
- Understand Vector calculus and Linear Algebra for solving Regression problems
- Solve Dimensionality reduction and Density estimation problems using Probability and Distributions

Pedagogy: The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations and quizzes. Faculty members strive to make the classes interactive so that students can correlate the theories with practical examples for better understanding. Use of ICT, web-based resources as well as flipped class room teaching will be adopted.

CONTENTS

UNIT 1	**12 Hours**
Introduction and Motivation - Linear Algebra Basics: Vector Spaces- Groups and Vector Subspaces; Basis - Generating Set and Basis; Linear Mappings- Matrix Representation of Linear Mappings **Matrix Decompositions:** Eigenvalues and Eigenvectors; Singular Value Decomposition (SVD)- Geometric Intuitions for SVD, Construction of SVD	
UNIT 2	**10 Hours**
Calculus: Partial Differentiation - Basic Rules of Partial Differentiation, Chain Rule; Gradients- Gradients of Vector-Valued Functions, Jacobian; Backpropagation- Gradients in a Deep Network, Automatic Differentiation	
UNIT 3	**10 Hours**
Probability and Distributions: Probability Space; Conditional Probability, Bayes theorem, Independence, Theorem of total probability, Mean and variance, Few Discrete and Continuous distributions, Joint distributions and Covariance	
UNIT 4	**10 Hours**
Optimization: Optimization using Gradient Descent - Learning rate, Gradient Descent with Momentum, Stochastic Gradient Descent; Constrained Optimization; Convex Optimization- Linear programming, Quadratic Programming	

Text Books
1. Marc Peter Deisenroth, A. Aldo Faisal, Cheng Soon Ong, Mathematics for Machine learning, Cambridge University Press, 2020.
2. Charu C. Aggarwal, Linear Algebra and Optimization for Machine Learning A Textbook, Springer International Publishing, 2020.

Reference Books
1. Vaisman, Radislav, et al. Data Science and Machine Learning: Mathematical and Statistical Methods. United States, CRC Press, 2019.

CYBER RISK MANAGEMENT	
Course Code: MIS-108 Contact Hours: L-3 T-1 P-0 Course Category: DEC	Credits: 4 Semester: 2

Introduction:

Cybersecurity risk management guides a growing number of IT decisions. Cybersecurity risks continue to have critical impacts on overall IT risk modeling, assessment and mitigation. There is a need to understand Cyber Security Risk and how it affects organization. Cyber Security Risk management is becoming a key requirement for any organization so as to enable them to help their organisations be better prepared and more resilient against cyber threats and attacks.

Course Objectives:

- Understand the Current Threat Landscape and Organizational risk trends
- Understand Cyber Risk Management Fundamentals and Identify Risks
- Understand Risk Management Life Cycle, Risk Mitigation, Risk Avoidance, Risk Transference, Risk Acceptance and Risk Rejection

Pre-requisite: Cyber Security Fundamentals

Course Outcome:

On successful completion of this course, students will be able to:

- Cyber security risk management framework and methodologies
- Identifying and modelling information security risks
- Qualitative and quantitative risk assessment methods
- Articulating cyber security risks as business consequences

Pedagogy:

The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations and quizzes. Faculty members strive to make the classes interactive so that students can correlate the theories with practical examples for better understanding. Use of ICT, web-based resources as well as flipped class room teaching will be adopted.

Contents

UNIT-I	10 Hours
Evolution of Information Security, **The Current Cyberspace Environment:** Introduction to Cyber Risk, Developing Awareness of the Cyber Threat, How Digital transformation impacts cyber security, privacy and security, new cyber trends, Cyber Threat landscape	
UNIT-II	10 Hours
Cyber Risk Fundamentals, Why is Cyber Risk important, Determining Risk, Risk Management Process, Quantitative vs Qualitative Risk Management, Risk Management Life Cycle, Frameworks and Methodologies, Risk Management Controls, Common Tools, Risk Management Assessment, Threat and Vulnerability Identification, Likelihood and Impact analysis	
UNIT-III	10 Hours

Risk Mitigation, Risk Avoidance, Risk Transference, Risk Acceptance and Risk Rejection, Introduction to Threat Modelling, How to Threat Model, Diagramming your Threat Model, Reduction Analysis, Defining Information Security Metrics, Analysis Techniques, Automating Metrics Calculation and Tools, Risk & Compliance Management, Risk Management, Information Security Standards, IPR, ISO/IEC 2700, HIPAA, COBIT, ISO 27001, PCIDSS, ISO 22301, NIST, Indian IT ACT and Standards.	
UNIT-IV	10 Hours
Data Protection and Data Privacy, Breach Response & Recovery, Cyber Crisis Management, Business Continuity Planning, Identifying Business Continuity requirements, Business Impact analysis, Planning your Continuity, BCP Components, Cost-Benefit Analysis, Availability and Reliability, Risk Evaluation, Business Consequences, Management Consulting Techniques, Industry Case Studies	
Text Books	
1. A.Refsdal, B. Solhaug, K. Stolen, “ Cyber-Risk Management”, Springer, 2015/Latest Edition.	
2. E. Wheeler, “Security Risk Management”, O’Reilly, 2011/Latest Edition.	
Reference Books	
1. R. Bentham, “Cyber Risk Management: Practical Strategies to Protect your Organization from Cyber Threats”, Kogan Page, 2018/Latest Edition.	
2. C.J. Hodson, “Cyber Risk Management: Prioritize Threats, Identify Vulnerabilities and Apply Controls”, Kogan Page, 2019/Latest Edition.	

CRYPTOGRAPHIC PROTOCOLS AND ALGORITHMS	
Course Code: MIS-110 Contact Hours: L-3 T-1 P-0 Course Category: DEC	Credits: 4 Semester: 2

Introduction:

This advanced course will introduce students to the application of cryptography in real world. The intent of this course is to familiarize students with various classical and modern cryptographic protocols that are widely-used, heavily analysed and accepted as secure. The focus will be on how to design protocols that perform security related function by applying cryptographic methods and primitives and are robust and resistant to attacks

Course Objectives:

- To acquire knowledge on standard cryptographic protocols that are used to provide confidentiality, integrity and authenticity
- To explain and use modern cryptographic methods (hybrid encryption, key management, hybrid digital signatures, mutual authentication)
- To understand wide variety of cryptographic protocols that go beyond the traditional goals of data confidentiality, integrity, and authentication to also secure a variety of other desired characteristics of computer-mediated collaboration

Pre-requisite: Fundamentals of Information Security

Course Outcome:

On successful completion of this course, students will be able to:

- Learn applied cryptographic basics and apply to real world problems
- Students will be able to select the right algorithm, protocol, and systems to develop secure systems to protect digital assets in the cyber world.
- Students will learn advanced security concepts such as secret sharing, how to provide ownership without revealing personal credentials, how to prove data existed at a certain time, auditable voting systems, commitment protocols etc.
- Students will learn interactive protocols that allow the signer to prove a forgery and limit who can verify the signature.

Pedagogy:

The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations and quizzes. Students would be encouraged to develop an understanding of various cryptographic concepts. Course will have a blend of theory and practical for the benefit of students. Use of ICT, web based sources and blended teaching will be adopted.

Contents

UNIT-I	10 Hours
Protocol Building Blocks, Communication Using Symmetric Cryptography, One Way Hash Functions, Communication using Public Key Cryptography , digital signatures, signature with encryption, Random and Pseudo random sequence generation, Basic Protocols: key exchange, Interlock Protocol, Key Exchange with Digital Signatures, Key and Message Broadcast, Basic Protocols: Authentication using hash functions, Authentication using public key cryptography.	
UNIT-II	11 Hours
Mutual Authentication, SKID and SKID 3, Wide Mouth Frog Protocol, Yahalom Protocol, Needham-Schroeder Protocol, Kerberos , DASS, Woo-Lam Protocol, Formal analysis of Authentication and Key exchange protocols, BAN Logic, Multiple Key Public Key Cryptography, Secret Splitting, Secret Sharing, LaGrange Interpolating Polynomial Scheme, Asmuth-Bloom, Secret Sharing with cheaters.	
UNIT-III	11 Hours
Intermediate Protocols: Time stamping services, Arbitrated Protocol, Linking Protocol, subliminal channels, Elgamal Subliminal Channel, Undeniable Digital signatures: Chaum protocol, Proxy signatures, Group signatures, Bit Commitment using symmetric cryptography, Bit Commitment using hash functions, fair coin flips, coin flipping protocol using hash functions and public key cryptography, key escrow.	
UNIT-IV	10 Hours
Advanced Protocols: Zero knowledge proofs, Zero knowledge proof for identity, Interactive ZKP: Graph Isomorphism, Hamiltonian Cycles, Non-interactive Zero knowledge proof, blind signatures, identity based public key cryptography, Oblivious transfer, oblivious signatures, Simultaneous contact signing, Digital certified Mail, Esoteric protocols, secure elections.	
Text Books	
1	W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, 7th Ed., 2017.
2	B. Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C, John Wiley & Sons, 2nd Ed., 2015.
3	Bernard Menezes, Network Security and Cryptography, Cenege Learning, 2nd Ed., 2012.
Reference Books	
1	A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC press, Hardcover Edition, 2018.
2	Dong, Ling, Chen, Kefei, Security Analysis Based on Trusted Freshness, 1st Ed., Springer, 2012.
3	Johannes Buchman, Introduction to Cryptography, 2nd Ed., Springer, 2012.

SECURITY PATTERNS			
Course Code	: MIS-112	Credits	: 4
Contact Hours	: L-3 T-0 P-2	Semester	: 2
Course Category	: DEC		

Introduction:

This course is designed to enable students to recognize the need for building a secure system in which security is an integral part of software lifecycle.

Course Objectives:

- To learn Software Development and Deployment that is reliable, scalable and portable.
- To learn object oriented programming through Security Design Patterns.
- To learn secure integrating web applications developed on varied platform through security patterns.

Pre-requisite:

Basic Knowledge of Object Oriented programming, Design patterns and Database Management

Course Outcome:

On successful completion of this course, students will be able to:

- Acquire Software development skills that are reliable, scalable and portable applications.
- Design and implement software development with Clean Code through use of Security Design patterns.
- Build complex systems with secure and reliable components.

Pedagogy

The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations and quizzes. Students would be encouraged to develop an understanding and implementation of various security patterns. Use of ICT and web based sources by using blended mode will be adopted.

Contents

UNIT-I	**10 Hours**
Introduction to Security patterns, Nature and need of security patterns, evaluation of secuirty patterns and their effect on security, Anatomy of security patterns, Characteristics of security patterns, uses of security patterns, classification of security patterns	
UNIT-II	**11 Hours**
Security Pattern Landscape, Circle of Trust, Security Needs Identification for Enterprise Assets, Threat Assessment, Vulnerability Assessment, Identification & Authentication (I&A) Requirements and Patterns, Patterns for Access Control: Authorization, Role-Based Access Control, Multilevel Security, Reference Monitor, Role Rights Definition, Implementation of Authentication and Authorisation patterns Using a case study.	
UNIT-III	**10 Hours**
System Access Control Architecture: Access Control Requirements, Single Access Point, Check Point, Security Session, Full Access with Errors, Limited Access, Implementation using web based application.	
UNIT-IV	**11 Hours**
The Implementation-Level Patterns: Secure logger and Auditor, Clear Sensitive Information, Secure Directory, Input Validator, Pathname Canonicalization Implementation of Patterns using web based application.	
Text Books	
1	Eduardo Fernandez, “Security patterns in Practice”, Wiley , First Edition, 2013
2	Markus Schumacher Eduardo Fernandez et al., “Security Patterns Integrating Security and Systems Engineering”, Wiley, 2006
Reference Books	
1	Ben Edmunds, “Securing PHP Apps”, Apress, 2016
2	Chad Dougherty, Kirk Sayre, Robert C. Seacord, David Svoboda, Kazuya Togashi “Secure Design Patterns”, Software Engineering Institute, CERT, First Edition, 2009

Applications of Machine Learning in Cyber Security	
Course Code: MIS 114 Contact Hours: L-3 T-0 P-2 Course Category: DEC	Credits: 4 Semester: 2

Introduction: We are witnessing numerous attacks on cyber systems. In this course, we shall study application of machine learning, the most popular branch of artificial intelligence, to detect attacks in cyberspace, thereby equipping the students with an important perspective to secure cyber systems.

Course Objective:

- Introduce cyber systems in different domains with the objective of securing cyber systems using machine learning.
- Help the students to engineer and build a secure cyber system using machine learning and deep learning.

Pre-requisite: Programming, Machine Learning.

Course Outcome: Upon successful completion of this course, students will be able to:

- Understand the key features (aspects) to extract from cyber systems from a security perspective.
- Apply the concepts of machine learning to secure cyber systems.

Pedagogy: The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations and quizzes. Faculty members strive to make the classes interactive so that students can correlate the theories with practical examples for better understanding. Use of ICT, web-based resources as well as flipped classroom teaching will be adopted.

Course Details:

UNIT I	**10 hours**
Introduction: Need for Machine Learning in Cyber Security. **Network Security:** NetFlows, BotNets, BotNet Detection. Deep Packet Inspection. Intrusion Detection. Anomaly Detection.	
UNIT II	**10 hours**
Behavioral Biometrics: Keyboard & Mouse Pattern Analysis, Active authentication. **Mobile Security:** Static & Dynamic Analysis, Malware Detection.	
UNIT III	**12 hours**
Web Security: Web Server Log Analysis, Email Spam Detection, Malicious URLs Detection, Phishing Attack Detection.	

UNIT IV	**10 hours**
Model Security: Data Poisoning Attacks, Generative Adversarial Networks. Deep Fakes - Creation and Detection. Dataset Inference. Model Reconstruction Attacks.	
Text Books	
1	Marcus A Maloof, “Machine Learning and Data Mining for Computer Security: Methods and Applications”, Springer, 2006..
2	Sushil Jajodia & Daniel Barbara, “Applications of Data Mining in Computer Security”, Springer, 2008.
Reference Books	
1	Dhruba Kumar Bhattacharyya & Jugal Kumar Kalita, “Network Anomaly Detection: A Machine Learning Perspective”, Chapman and Hall/CRC; 1st Edition, 2013.

ADVANCED NETWORK TECHNOLOGY	
Course Code: MIS-116 Contact Hours: L-3 T-0 P-2 Course Category: DEC	Credits: 4 Semester: 2

Introduction:

This advanced course develops knowledge about networks to understand their complexity and inform their future design. It seeks to discover and understand common principles and fundamental structures underlying networks and their behaviours. It makes students familiar with the foundations of computer networking, network protocol design and performance evaluation/analysis, and recent advances in network architecture and technology.

Course Objectives:

- To give the students an understanding of the principles behind the latest advances in computer network technology, from IPv6 extending to pervasive and ubiquitous computing
- To develop familiarity with current research problems and research methods in advance computer networks

Pre-requisite: Computer Networks

Course Outcome:

On successful completion of this course, students will be able to:

- Illustrate reference models with layers, protocols and interfaces. Summarize functionalities of different Layers.
- Combine and distinguish functionalities of different Layers and understand principles behind the latest advances in advanced network technology.
- Describe and Analysis of advanced protocols of computer networks, and how they can be used to assist in network design and implementation.

Pedagogy:

The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations and quizzes. Students would be encouraged to develop an understanding of advanced networking concepts and their implementation for real world problems. Use of ICT and web based sources by using blended mode will be adopted.

Contents

UNIT- I	10 Hours
TCP/IP Protocol Architecture, OSI Model, Error detection and correction, Medium Access, Flow and Error Control, Noiseless Principles of Internetworking, Internet protocol operation, IPV4:ICMP, ARP, RARP, IPV6, IGMP, Interior Routing protocols, Exterior Routing Protocols, ARQ, TCP, UDP, Congestion control and Flow Control, Overview of QoS, Integrated Services, Differentiated Services	
UNIT-II	10 Hours
IEEE 802.11a/b/n/g/p, 802.15, and 802.16 standards for Wireless PAN, LAN, and MAN, IPv6 – Header, Addressing, Neighbour Discovery, Auto-Configuration, Header Extensions and options, support for QoS, security, etc., DHCPv6, Mobile Ipv6 rationale and operation – intra and inter site IP, Multicasting: Multicast routing protocols, Virtual private network service, Multiprotocol label switching (MPLS)	
UNIT-III	10 Hours
Wireless Sensor Networks, Wireless Body Area Networks, Mobile Ad Hoc Network, Vehicular Adhoc Network, Data Center Networking, Delay Tolerant Networking, Home Networking, Green Networking, Internet of Things, Software Defined Networking, Web- Scale Networking: Distributed Cloud Computing and Virtual Machine Migration.	
UNIT-IV	10 Hours
Content Networks: Video Streaming, Wireless Networking: Wireless Mesh, Geographic Routing, Network Security principles, Security related issues in wireless networks, Public and Private Key Cryptography, Key distribution protocols. Digital Signatures, and digital certificates, Firewall, Next Generation Fire wall, **Radio Networks, Opportunistic Network**	
Reference Books	
1. W. R. Stevens. TCP/IP Illustrated, Volume 3: TCP for Transactions, HTTP, NNTP, and the Unix Domain Protocols, Addison Wesley, 2016.	
2. W. Stallings. Data and Computer Communications, 10th Edition, Pearson, 2013.	
3. J Kurose and KW Ross. Computer Networking: A Top-Down Approach, 7th Edition, Pearson, 2017	
Text Books	
1. W. Stallings. Cryptography and Network Security: Principles and Practice, 7th Edition, Prentice Hall, 2016.	
2. Ibrahiem M. M. El Emary, S. Ramakrishnan, Wireless Sensor Networks: From Theory to Applications, 1st Edition, CRC Press, 2013	

CYBER LAWS AND RIGHTS	
Course Code: MIS-118 Contact Hours: L-3 T-1 P-0 Course Category: DEC	Credits: 4 Semester: 2

Introduction:

The objective of this course is to enable students to understand, explore, and acquire a critical understanding of cyber law. Develop competencies for dealing with frauds and deceptions (confidence tricks, scams) and other cybercrimes. It also covers overview of Intellectual Property Right and Cyber Laws in Indian and global perspectives.

Course Objectives:

- To introduce the cyber world and cyber law in general
- To explain about the various facets of cyber crimes
- To enhance the understanding of problems arising out of online transactions and provoke them to find solutions
- To clarify the Intellectual Property issues in the cyber space and the growth and development of the law in this regard
- To educate about the regulation of cyber space at national and international level

Pre-requisite: Cyber Security Fundamentals

Course Outcome:

On successful completion of this course, students will be able to:

- Understand the cyber world and cyber law in general and various facets of cyber crimes
- Understand regulation of cyber space at national and international level
- Understand the Intellectual Property issues in the cyber space

Pedagogy:

The teaching-learning of the course would be organized through lectures, assignments, projects/presentations and case studies. Students would be encouraged to develop an understanding of cyber laws and cyber rights. Use of ICT and web based sources by using blended mode will be adopted.

Contents

UNIT-I	10 Hours
Cyber World: An overview, The internet and online resources, Security of information, Digital signature, Cyber Law: An Overview, Introduction about the cyber space, Regulation of cyber space – introducing cyber law, Scope of Cyber laws – e-commerce; online contracts; IPRs (copyright, trademarks and software patenting); e-taxation; e-governance and cyber crimes, Cyber law in India with special reference to Information Technology Act, 2000	
UNIT-II	10 Hours
Computer crime and cyber crimes; Classification of cyber crimes, Distinction between cyber crime and conventional crimes, Reasons for commission of cyber crime, Cyber forensic, Cyber criminals and their objectives, Kinds of cyber crimes – cyber stalking; cyber pornography; forgery and fraud; crime related to IPRs; Cyber terrorism; computer vandalism etc. Regulation of cyber crimes -Issues relating to Investigation, Issues relating to Jurisdiction, Issues relating to Evidence, Relevant provisions under Information Technology Act, 2000, Indian Penal Code, Pornography Act and Evidence Act etc., Plagiarism Issues, Tools to detect Plagiarism, Plagiarism Tools : Turnitin, Viper	
UNIT-III	10 Hours
Online business- Definition of E-commerce, Types of E-commerce, Important Issues in Global E-commerce (Issues relating to Access (to infrastructure; to contents; universal access; Digital Divide and Universal Divide); Trust, Privacy; Security; Consumer Protection; Content Regulation; Uniformity in Legal Standards pertaining to internet), Application of conventional territory based law to E-commerce (Taxation, Intellectual Property Rights, International Trade, Commercial law and standards, Dispute resolution) IPR – An Overview, Copyright Issues in Cyberspace (Linking, Inlining, Framing, Protection of content on web site, International Treaties), Trademark Issues in cyberspace (Domain Name Dispute, Cybersquatting, Uniform Dispute Resolution Policy, Meta-tags and Key words), Computer Software and Related IPR Issues	
UNIT-IV	10 Hours
Data Protection Laws, Indian evidence act, Examiner of Electronic evidence, amendments introduced in Indian evidence act, Indian CERT, Law regarding Electronic Cheques and truncated cheques, IT rules 2000, Ministerial Order on blocking of websites, Cyber laws in Global Prospective	
Text Books	
1. Prashant Mali, Cyber Law & Cyber Crimes Simplified, Fourth Edition, Snow White Publications, 2017.	
2. Vakul Sharma, Information Technology - Law and Practice (Law and Emerging Technology, Cyber Law & E-Commerce), Sixth Edition, Universal Law Publishing Co. (ULPC), 2018.	
3. Pavan Duggal, Textbook on Cyber Law, 2nd Edition, Universal Law Publishing, 2016.	
4. Matthew Richardson, Cyber Crime: Law and Practice, Second Edition, Wildy, Simmonds and Hill Publishing, 2019.	

SECURITY AND PRIVACY IN ONLINE SOCIAL NETWORKS	
Course Code: MIS-120 Contact Hours: L-3 T-1 P-0 Course Category: DEC	Credits: 4 Semester: 2

Introduction

Social Media is playing a significant role and affecting the online user behaviours in many ways. The primary motivations for users to join social media platforms are to share information, connect to their friends and engage with them. On one hand social media offers these advantages, however, on other hand, the issues of privacy and security are also getting manifested in various forms. And, given that we all are using one (or more) social media platforms, it is important for all of us to learn these issues of privacy and security arising out of social media so that we remain safe online.

Course Objectives

- Understand the fundamentals of social media
- Collect social media data as a developer
- Learn challenges in social media related to privacy and security

Pre-requisites

- Knowledge of object oriented programming principles
- Basic understanding of Machine Learning

Course Outcome

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

- Understand security and privacy challenges in any social media platform
- Develop automated systems to solve security and privacy problems

Pedagogy

Lectures will be supported with case studies (driven by research papers) of privacy and security problems in social media. Emphasis will be on practical system development by writing programs to collect, analyze and infer insights from social media

Contents

<table>
<tr><td colspan="2">UNIT-I</td><td>10 Hours</td></tr>
<tr><td colspan="3">Social Media - Introduction; Social Media - User vs Developer’s Perspective, Data Collection APIs; Social Media Content Analysis - BoW Model, TF-IDF; Network Analysis - Node Centrality Measures, Degree Distribution, Average Path Length, Clustering Coefficient, Power Law; Synthetic Networks - Random Graphs, Preferential Attachment Model.</td></tr>
<tr><td colspan="2">UNIT-II</td><td>11 Hours</td></tr>
<tr><td colspan="3">Security Issues in Social Media - Overview; Review of Machine Learning; Identity Theft - Profile Cloning, Social Phishing; Fake, Compromised, Sybil accounts and their behavior; Spamming; Rumour or Misinformation; Cyberbullying; Collective Misbehaviors.</td></tr>
<tr><td colspan="2">UNIT-III</td><td>11 Hours</td></tr>
<tr><td colspan="3">Privacy Issues in Social Media - Overview; Privacy Settings; PII Leakage, Identity vs Attribute Disclosure Attacks; Inference Attacks; De-anonymization Attacks; Privacy Metrics - k-anonymity, l-diversity; Personalization vs Privacy, Differential Privacy.</td></tr>
<tr><td colspan="2">UNIT-IV</td><td>10 Hours</td></tr>
<tr><td colspan="3">Social Media Case Studies - Facebook, Twitter, Instagram, YouTube, LinkedIn, StackOverflow, GitHub, Quora, SnapChat, Reddit, FourSquare, Yelp.</td></tr>
<tr><td colspan="3">Text Books</td></tr>
<tr><td>1</td><td colspan="2">Zafarani, Reza, Mohammad Ali Abbasi, and Huan Liu. Social media mining: an introduction. Cambridge University Press, 2014.</td></tr>
<tr><td colspan="3">Reference Books</td></tr>
<tr><td>1</td><td colspan="2">Bonzanini Marco. Mastering Social Media Mining. Packt Publishing, 2016.</td></tr>
<tr><td>2</td><td colspan="2">Mikhail Klassen, Matthew A. Russell. Mining the Social Web. 3rd Edition. O’Reilly Media, Inc, 2019</td></tr>
</table>

SOFTWARE DEFINED NETWORKS	
Course Code: MIS-122	Credits: 4
Contact Hours: L-3 T-1 P-0	Semester: 2
Course Category: DEC	

Introduction:

This course introduces software defined networking, an emerging paradigm in computer networking that allows a logically centralized software program to control the behaviour of an entire network.

Course Objectives:

- Differentiate between traditional networks and software defined networks
- Understand advanced and emerging networking technologies
- Obtain skills to do advanced networking research and programming
- Learn how to use software programs to perform varying and complex networking tasks
- Expand upon the knowledge learned and apply it to solve real world problems

Pre-requisites:

Basic understanding of data communication and computer networks

Course Outcomes:

On completion of the course, students will be able to:

- Understand the functionalities of core SDN and its applications
- Get an exposure of SDN programming frameworks

Pedagogy:

The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations and quizzes. Students would be encouraged to develop an understanding of SDN and related technologies. Use of ICT and web based sources by using blended mode will be adopted.

Contents

UNIT-I	10 Hours
Introduction: Evolution of networking technology, Forerunners of SDN, SDN origins and evolution – Why SDN? Evolution of switches and control planes Centralised and Distributed control and data planes, The genesis of SDN, Software Defined Network software stack	
UNIT-II	10 Hours
SDN architecture: How SDN works? ForCES and Open Flow control. SDN controllers: Introduction-general concepts. **Network virtualization:** Network programmability-NetApp development, Network slicing.	
UNIT-III	8 Hours
SDN applications: SDN solutions for data centre networks-use cases and applications, Open network operating system SDN applications in wireless networks and IoT-case studies and applications.	
UNIT-IV	12 Hours
Implementing SDN: Juniper SDN Framework-IETF SDN Framework- Open Daylight Controller-Floodlight Controller-Bandwidth-Calendaring-Data Center Orchestration **SDN future and challenges:** Control and data plane scalability, Security, Fault tolerance, Enhancing the data plane: OpenFlow++	
Text Books	
1	SDN - Software Defined Networks by Thomas D. Nadeau & Ken Gray, O'Reilly, 2013
2	Software Defined Networking with OpenFlow By Siamak Azodolmolky, Packt Publishing, 2013
References	
1	Software Defined Networks: A Comprehensive Approach by Paul Goransson and Chuck Black, Morgan Kaufmann Publications, 2014
2	Feamster, Nick, Jennifer Rexford, and Ellen Zegura. "The road to SDN: an intellectual history of programmable networks." ACM SIGCOMM Computer Communication Review 44.2 (2014): 87-98.
3.	Kreutz, Diego, et al. "Software-defined networking: A comprehensive survey." Proceedings of the IEEE 103.1 (2015): 14-76.
4.	Nunes, Bruno AA, et al. "A survey of software-defined networking: Past, present, and future of programmable networks." Communications Surveys & Tutorials, IEEE 16.3 (2014): 1617-1634.

Research Methodology and Publication Ethics	
Course Code: ROC 902 Contact Hours: L-3 T-1 P-0 Course Category: M.Tech/Ph.D	Credits: 4 Semester: 1/2

Introduction: An M.Tech/ Ph. D. may become an Instructor/Mentor/Facilitator in an Academic Institute or a Researcher in some Industry/Institute. This course is a foundation to let her optimize the time spent in research during and after M.Tech/Ph. D programme.

Course Objectives:

- To familiarize with the various steps in research.
- To familiarize with global standards in research world.
- To familiarize with global & domestic industry trends
- To familiarize with Product oriented research
- To enable the student to think rationally to formulate and solve a problem to the ultimate benefit of the society and welfare of mankind

Pre-requisites: None

Course Outcomes:

Having successfully completed this course, the student will be able to

- Gain knowledge and comprehend various fundamentals of research.
- Build a sound foundation of methodologies and applications of research.
- Identify and analyze relationship between technical/multidisciplinary areas and integrate them for various applications.
- Evaluate and apply the quantitative and qualitative aspects of research to innovate devices and processes in the constantly competitive Technologies.
- Identify and evaluate the Cross functional coalition aspects
- Know how on how to take research to a product implementation

Pedagogy:

Classroom teaching which focuses upon relating the textbook concepts with real world phenomena, along with case studies.

UNIT-I	10 Hours
Research: Types of Research, Research problem and hypothesis formulation, Systematic vs. Meta-analysis **Peer Review:** Stewardship of Data. Research Metrics. Research Indices. **Meta Research**: Impact Factor, H index, SNIP, SJP, SJR, CiteScore , EigenFactor, Article influence score, Altimetric. **Standards**: DOI, ISO, ISSN, ISBN. **Citation databases:** Web of Science, Scopus, ICI	
UNIT-II	11 Hours
Publication: Authorship. Conferences. Open Access. Research Report and Research paper **Writing:** Organizing research work into different sections of a research Paper. **Research Design**: Sampling Design, Data Collection and Measurement, Data analysis using R. **Hypothesis Testing:** Selection of Variables, Z-test, t-test, ANOVA.	
UNIT-III	11 Hours
Ethics: Ethical Theories: Virtue Ethics, Kant, Kohlberg Moral Development, Epistemology, Research on Human subjects, Nuremberg Code, Declaration of Helsinki. **Scientific Misconduct**: Plagiarism, COPE, WAME. **Law**: Patent Act, Copyright Act. Conflict of Interest. Sarbanes Oxley Act.	
UNIT IV	10 Hours
Case studies: Milgram experiment, Stanford prison experiment, Henrietta Lacks, Plutonium experiment, Tuskegee Syphilis Experiment, and Plastic Fantastic. The case studies are not limited to these. The instructor may include more as per the contemporary cases. **Stress Management:** Interpersonal Skills. Team Work.	
Books	
1	C R Kothari and Gaurav Garg, Research Methodology: Methods and Techniques, New Age International Publishers (2019)
2	Machedo, Research Methodology in Management and Industrial Engineering, Springer, 2020
3	Gatrell, Research design and proposal writing in spatial science, , Springer, 2020
4	Deb, Engineering Research Methodology A Practical Insight for Researchers, Springer, 2019

Ethical Hacking	
Course Code: MIS 201 Contact Hours: L-3 T-0 P-0 Course Category: DEC	Credits: 3 Semester: 3

Introduction: In lieu of the fact that most of the official work (private and public) is done through computer and computer systems, it is important to ensure security in such cases. All the necessary documents, information, and data are stored in a computer these days which should be protected with utmost care. Following this, there is a lot of demand for ethical hacking professionals to keep all the sensitive information protected from the hackers and develop new computer protecting the system. In this course, students will taught how to find loopholes in the security system and how to report these threats to their owners and provide necessary solutions to protect the data and networks.

Course Objective: To acquire knowledge on about various security threats that exist and can be exploited

- To learn how bots, botnets, viruses, worms, Trojans, DOS attacks, DDOS attacks etc. work and are utilized for hacking
- To learn various ethical laws that exist in India and abroad and their significance
- To understand how loopholes and potential risks can be detected and learn wide variety of solutions that can be applied to protect data and networks.

Pre-requisite: None

Course Outcome: On successful completion of this course, students will be able to:

- Learn Ethical hacking tools and techniques
- Learn aspects of security, importance of data gathering, foot printing and system hacking.
- Analyze how intruders escalate privileges?
- Learn and analyze advanced concepts such as DDoS Attacks, Buffer Overflows, SQL Injection, Cross Site Scripting, Virus Creation
- Develop technical and analytical skills with in-depth knowledge of ethical hacking concepts that will assist them to take certification exam in future
- Apply and use ethical hacking techniques to real world problems
- Design and develop new simple ethical hacking algorithms to solve real world security challenges

Pedagogy: The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations and quizzes. Students would be encouraged to develop an understanding of the existing real life cyber security issues and how they are solved. Use of ICT and web based sources by using blended mode will be adopted.

Contents

UNIT-I	7 Hours
Introduction to Ethical Hacking, Hacking Laws, Foot-printing, Reconnaissance,, Scanning, System hacking Cycle, Enumeration, Cracking Password, Types of password attacks, Trojans and Backdoors, Types of Trojans, Viruses, Worms, Rootkits	
UNIT-II	7 Hours
Sniffers, Types of Sniffing, Phishing, Methods of Phishing, Types of Phishing Attacks, Process of Phishing, Denial of Service, Classification of DoS attacks, Bots and Botnets, Botnets Life Cycle, System and Network Vulnerability.	
UNIT-III	7 Hours
Ping of Death attack, Session Hijacking, Spoofing vs Hijacking, Session Hijacking Levels, Network Level Hijacking, 3 way handshake, IP Spoofing, RST Hijacking, TCP/IP Hijacking,	

SQL Injection, Cross Site Scripting.	
UNIT-IV	7 Hours
Dark web, Darknet and Tor, Layers of Web, Uses of Deep Web, Ethical Uses of Darknet, How to Access Darknet Safely, Accessing the Deep Web Authentication: RSA SecurID Token, Biometrics, Hacking Wireless Networks, Tools for ethical hacking.	
Text Books	
1	S. McClure, J. Scambray and G. Kurtz, Hacking Exposed 7: Network Security Secrets & Solutions, Tata Mc Graw Hill Publishers, 3rd ed., 2012.
2	Sean-Philip Oriyano, CEH v9: Certified Ethical Hacker Version 9 Study Guide, 1st Ed., Wiley & Sons, 2016.
Reference Books	
1	M.T. Simpson, N. Antill, “Hands-On Ethical Hacking and Network Defense”, 3rd Ed., Cengage Learning , 2016
2	Rafay Baloch, “A Beginners Guide to Ethical Hacking”, 1st Ed., CRC Press, 2014

Cloud Computing Architecture and Security	
Course Code: MIS-203 Contact Hours: L-2 T-0 P-2 Course Category: DEC	Credits: 3 Semester: 3

Introduction:

The course aims to familiarize the students with the advanced concepts of Cloud Computing Architecture and its Security Life Cycle. The prominent attributes of a secure cloud platform are data security, scalability, easy accessibility and sharing of data, zero maintenance, and easy data recovery. The course is designed for inculcating the research aptitude in graduate students, keeping the needs of Enterprise Cloud Computing in Industry 4.0 and the academic research.

Course Objectives:

- To comprehend importance of Enterprise Cloud Computing in Industry 4.0 and research
- To learn Cloud Computing architecture, its Security Requirements and Virtualization
- To understand Cloud Computing Life Cycle Management and Provisioning
- To identify current Security Challenges in Enterprise Cloud Computing

Pre-requisites:

Basic understanding of Operating System, Network Security, Parallel and Distributed Computing, Computer Organization and Architecture

Course Outcome:

- Conceptual clarity in Grid and Cloud Computing architecture
- Conceptual understanding of Virtualization at different levels
- Logical insight for comprehending the Security Primitives in Cloud Computing
- A Research Case Study identifying Security Objectives and proposing a relevant solution

Pedagogy:

The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations and quizzes. Faculty members strive to make the classes interactive so that students can correlate the theories with practical examples for better understanding. Use of ICT, web-based resources as well as flipped classroom teaching will be adopted.

Contents

Unit - I	**7 Hours**
Introduction: Introduction of Cloud Computing (CC), NIST definition of CC, Peer-to-Peer Approach, Parallel-Distributed Computing, Cluster and Grid Computing, Autonomic and Utility Computing, Platform Virtualization, Service Oriented Architecture, Significance of CC Paradigm in Industry 4.0, Advantages, Disadvantages and Limitations of CC. **Cloud Architecture and Service Models:** Cloud Dynamic Infrastructure and Architecture, Cloud Life Cycle Management, Service Models of CC: SaaS, IaaS, PaaS, CaaS, CC Sub-Service Models, Deployment Models of Cloud: Public, Private, Community Clouds, Linthicum Cloud Deployment	

Model, Jericho Cloud Cube Model, CC Sub-Service Models, Cloud Deployment Models: Public, Private, Community Clouds, Linthicum and Jericho Cloud Cube Deployment Model.	
Unit - II	**8 Hours**
Basics of Virtualization: Introduction of Virtualization & its need, Types of Virtualization, Virtual Clusters, Virtualization Reference Model, Advantages and Limitations of Virtualization, Techniques used for computing Virtualization, Logical Partitioning, Hypervisor Taxonomy, Concept of Virtual Machine, Hardware Virtual machine, Virtualization at Server End, Virtualization at Desktop End, Network Virtualization and Data Center Virtualization. **Concepts in Virtualization:** Virtualization Reference Model, Server/Compute Virtualization (at Server) and its Components, Techniques and Components for Desktop Virtualization, Features of Desktop Virtualization Drivers, Components of Network Virtualization: Virtual Switches and Virtual LAN, Traffic Management and its Techniques, Virtual Machine Migration Services, Virtual Machine Provisioning and Migration Services Management.	
Unit - III	**8 Hours**
Cloud Data Center: Core elements of Cloud Data Center, Storage Network Technologies and Virtualization, Object-based Storage Technologies, Unified Storage, RAID Technology and its Advantages, Technologies of Backup and Disaster Recovery, Replication Technologies, Cloud Data Center Management, Information Life Cycle Management, Cloud Analytics, Computing on Demand. **Introduction to Secure CC:** Overview of Data Security and Privacy, Security Concerns of CC, Security requirements for CC Architecture, Security Patterns and Architectural Elements, Cloud Security Design Principles, Cloud Security Architecture, Planning Strategies for Secure Operations, Data Encryption, Cloud Data Storage, Cloud Lock-in.	
Unit – IV	**7 Hours**
Advanced Security Issues: Security Concerns-Threats to Infrastructure, Data and Access Control, Cloud Information Security Objectives: Confidentiality, Accessibility, Organizational Security and Privacy Requirements, Cloud Security Design Principles, Secure Cloud Software Testing, Input Validation and Content Injection, Database Integrity Issues, Network Intrusion and Session Hijacking Attacks, Fragmentation Attacks, Secure Cloud Software Testing, Identity Management and Access Control, Information Privacy, Mobile Cloud Computing, Cloud Usage for Big Data Analytics and Internet of Things.	
Text Books	
1. Ronald L. Krutz, Russell Dean Vines, “Cloud Security: A Comprehensive Guide to Secure Cloud Computing”,Wiley-India 1st edition, 2010	
2. Barrie Sosinsky, “Cloud Computing Bible”, Wiley-India 1st edition, 2011	
3. Austin Young, Cloud Computing: A Comprehensive Guide to Cloud Computing, Independently Published, July-2019	
Reference Books	
1. Gautam Shroff, “Enterprise Cloud Computing Technology Architecture Applications” Cambridge University Press 1st edition, 2010	
2. Rajkumar Buyya, James Broberg, Andrzej M. Goscinski, “Cloud Computing: Principles and Paradigms”, Wiley-India , 2011	

3. Miller Michael, “Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online”, Pearson Education India ,1st edition, 2008
4. Ray J. Rafaels, Cloud Computing: From Beginning to End, Independently Published, April-2015

SECURITY TESTING AND RISK MANAGEMENT			
Course Code	: MIS-205	Credits	: 3
Contact Hours	: L-2 T-0 P-2	Semester	: 3
Course Category	: DEC		

Introduction: This course is designed to enable students to recognize the need for Security Testing of software applications and assessing the risk associated. Design software with a security mindset and implementing security by writing secure code does not necessarily meanthat the software is secure. It is imperative to validate and verify the functionality and security of software and this can be accomplished by quality assurance testing which should include testing for security functionality and security testing. Security testing is an integral process in the secure software development life cycle. Software that has undergone and passed validation of its security through testing is said to be of relative higher quality than software that hasn't. The course is effective in enabling students to learn Software Security testing techniques so as to develop software that is reliable and resilient to software attacks.

Course Objectives:

- To learn different types of functional and security testing and criteria that can be used to determine the type of security tests.
- To learn implementation of security patterns in removing the software and network vulnerabilities.
- To learn assessment and management of Risk through various risk assessment and management framework.

Pre-requisite:

- Basic Knowledge of Software applications, programming, Database, Network Concepts,

Course Outcome: Upon successful completion of this course, students will be able to:

- Learn what to test, which modules to test and how to test for software security issues.
- Perform Security testing of software and web applications.
- Detect Security vulnerabilities in software and network.
- Implement Security patterns and security controls to secure Software applications and network.
- Assess, evaluate and analyse risk of a software applications using standard Rsik assessment and Management Framework.

Pedagogy

Lectures will be imparted along with hands on lab sessions and security testing and risk management for software applications for case study (ies) .

Contents

UNIT-I	07 Hours
Introduction: Testing Objectives, Software Testing Process, Software Testing Principles, Tester Role in Software Development Organization, Test Case Implementation and Execution. Testing Concepts: Levels of Testing, Test Cases Design and Strategy, Test Suit, Test Plan, Testing as a Process, Security Testing Versus Traditional Software Testing, the Paradigm Shift of Security Testing, High-Level Security Testing Strategies, the Fault Injection Model of Testing	
UNIT-II	07 Hours
Software Vulnerabilities fundamentals: causes of software vulnerabilities, Software Vulnerabilities, Principle and Classification of software vulnerabilities, authentication and authorization, classification of SQL Injection attacks, distributed denial of service attacks, session attacks, Cross site scripting, Cross site request forgery (CSRF)	
UNIT-III	10 Hours
Security Testing into the Software Development Lifecycle, Need for Security Testing, Testing Techniques, Attack Surface Validation, Cryptographic Validation Testing, Penetration Testing, Testing for Input Validation, Testing for Scripting Attacks Controls, Network fault injection, port discovery, port scanning, proxies, Testing for Error and Exception Handling Controls, Vulnerability Detection and Assessment Approaches Software design Patterns and Security Patterns, their role, impact and usability. Tools for Security Testing	
UNIT-IV	06 Hours
Risk Management, Categories of Risk, Approaches to Risk Identification, Analyzing Risk, Qualitative Analysis and quantitative analysis, Performing Ongoing Risk Analysis, conducting Routine security review, Responding to Security Incidents, ranking the risk associated with a vulnerability, Vulnerability scoring system CVSS, Risk Prioritization, Planning the risk response, Updating Security Policy Case Study: Risk Assessment and Management Framework (Any One: OCTAVE-Allegro, OCTAVE-S, ISMS)	

Text Books	
1	Chris Wysopal, Luke Nelson and Elfriede Dustin, “ The Art of Software Security Testing, “Pearson Education, 2006
2	Alfred Basta, Nadine Basta, Mary Brown, “Computer Security and Penetration Testing”, Cengage India Private Limited, Second Edition, 2017
Reference Books	
1	Evan Wheeler, “Security Risk Management: Building and information Security Risk Management Programme from the Ground UP”, Syngress , 2011
2	Mano Paul, Official (ISC) 2 Guide to the CSSLP, CRC Press, First Edition, 2016

Natural Language Processing	
Course Code: MIS 207 Contact Hours: L-2 T-0 P-2 Course Category: DEC	Credits: 3 Semester: 3

Introduction: Natural Language Processing (NLP) is concerned with automatically processing human language. Applications include machine translation, search, automatic summarization, and dialog systems. NLP has proved to be a hard task, among other things because of the complexity of the structure of human language, and because of the massive amount of world knowledge that humans use in language understanding. This course provides a broad introduction to NLP with a particular emphasis on core algorithms, data structures, and machine learning for NLP.

Course Objectives:

- To describe the architecture of and basic design for a generic NLP system
- To discuss the current and likely future performance of several NLP applications, such as machine translation and Semantic analysis
- To briefly describe a fundamental technique for processing language for several subtasks, such as morphological analysis, syntactic parsing, word sense disambiguation etc
- To explain how NLP techniques draw on and relate to other areas of (theoretical) computer science, such as formal language theory, formal semantics of programming languages

Pre-requisite: Proficiency in at least one programming language

Course Outcome: Upon successful completion of this course, students will be able to:

- Identify and discuss the characteristics of different NLP techniques
- Identify and discuss the characteristics of machine learning techniques used in NLP
- Implement a hidden Markov model for part-of-speech tagging
- Understand what constitutes a probabilistic language model and understand the difference in assumptions between different types of such models (e.g. bag-of-words, n-gram, HMM, topic model)
- Create features for probabilistic classifiers to model novel NLP tasks

Pedagogy: The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations and quizzes. Faculty members strive to make the classes interactive so that students can correlate the theories with practical examples for better understanding. Use of ICT, web-based resources as well as flipped classroom teaching will be adopted.

Course Details:

UNIT I	**8 hours**
Introduction: Stages of NLP, N-grams, Words: Structure (Spellcheck, morphology using FSTs), Words: Semantics (Lexical Semantics, WordNet and WordNet based Similarity measures, Distributional measures of similarity, Concept mining using Latent Semantic Analysis), Word Sense Disambiguation (supervised, unsupervised and semi supervised approaches)	
UNIT II	**7 hours**
Words: Part of Speech (POS) tagging using Brill's Tagger and HMMs. Sentences: Basic ideas in compositional semantics, classical parsing (Bottom up, top down, Dynamic Programming, CYK Parser, parsing using probabilistic Context Free Grammars and EM based approaches for learning PCFG parameters.	
UNIT III	**8 hours**
Word Embeddings (Word2Vec, GloVe, LDA, TF-IDF), Skip-gram model, CBOW, Topic modelling: Latent Dirichlet Allocation, Gibbs sampling for LDA, LDA variations and applications, Semantic Analysis: Introduction, Affective lexicons (Learning and Computation), Language modelling: Basic ideas and smoothing techniques	
UNIT IV	**7 hours**
Information Extraction: Introduction to Named Entity Recognition and Relation Extraction, relation between Information Retrieval and NLP. Summarization (Single document, Multiple documents, query based), Question answering.	
Text Books	
1	Daniel Jurafsky and James H. Martin. Speech and Language Processing: An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition, Upper Saddle River, NJ: Prentice-Hall, 2nd Edition, 2009/ Latest Edition.
2	Natural Language Processing and Information Retrieval: Tanvier Siddiqui, U.S. Tiwary, Oxford University Press,2008/Latest Edition
Reference Books/Material	
1	Christopher D. Manning and Hinrich Schuetze. Foundations of Statistical Natural Language Processing. Cambridge, MA: MIT Press.Latest Edition.

2	Allen, J:” Natural Language Understanding.”. Latest Edition, The Benajmins/Cummings Publishing Company Inc. 1994. ISBN 0-8053-334-0
3	https://nptel.ac.in/courses/106/105/106105158/
4	https://nptel.ac.in/courses/106/106/106106211/

NEURAL NETWORKS AND DEEP LEARNING	
Course Code: MIS 209 Contact Hours: L-2 T-0 P-2 Course Category: DEC	Credits: 3 Semester: 3

Introduction:

Deep Learning has received a lot of attention over the past few years to solve a wide range of problems in Computer Vision and Natural Language Processing. Neural networks form the basis of deep learning. This course intends to cover fundamentals of neural networks, deep learning and application areas.

Course Objectives:

- To learn about the building blocks used in Deep Learning based solutions.
- Introduce major deep learning algorithms, the problem settings, and their applications to solve real world problems
- To understand various optimization algorithms which are used for training such deep neural networks.

Pre-requisites:

Working knowledge of Linear Algebra, Probability Theory. It would be beneficial if the participants have done a course on Machine Learning

Course Outcomes:

- Attain working knowledge of deep architectures used for solving various Vision and NLP tasks
- Identify the deep learning algorithms which are more appropriate for various types of learning tasks in various domains.
- Implement deep learning algorithms and solve real-world problems.

Pedagogy:

The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations and quizzes. Faculty members strive to make the classes interactive so that students can correlate the theories with practical examples for better understanding. Use of ICT, web-based resources as well as flipped classroom teaching will be adopted.

Contents

UNIT-I	7 Hours
Review of the Multi-Layer-Perceptron and Feedforward, Backpropagation algorithm. Gradient Descent (GD), Momentum Based GD, Nesterov Accelerated GD, Stochastic GD, AdaGrad, RMSProp. Case study: Malware classification	
UNIT-II	8 Hours
Unsupervised Learning, Singular Value Decomposition. Autoencoders and relation to PCA, Regularization in autoencoders, Regularization: Bias Variance Tradeoff, L2 regularization, Early stopping, Dataset augmentation, Parameter sharing and tying. Greedy Layerwise Pre-training, Better activation functions and weight initialization methods, Case study: Clustering Malware	
UNIT-III	7 Hours

Convolutional Neural Networks, state-of-the-art CNN models. Learning Vectorial Representations of Words. Recurrent Neural Networks, Backpropagation through time. Encoder Decoder Models, Attention Mechanism, Attention over images. Case study: Bytecode based malware detection	
UNIT-IV	8 Hours
Restricted Boltzmann Machines, Motivation for Sampling, Markov Chains, Gibbs Sampling for training RBMs, Contrastive Divergence for training RBMs. State-of-the-art transformer models. Case study: Malware analysis using Text Processing	
Text Books	
1	Deep Learning, An MIT Press book, Ian Goodfellow and Yoshua Bengio and Aaron Courville http://www.deeplearningbook.org, 2016
Reference Books	
1	A. Ravindran, K. M. Ragsdell , and G. V. Reklaitis , ENGINEERING OPTIMIZATION: Methods and Applications , John Wiley & Sons, Inc. , 2016

BLOCKCHAIN FUNDAMENTALS	
Course Code: MIS-211 Contact Hours: 2-0-2 Course Category: DEC	Credits: 3 Semester:3

Introduction: Blockchain can be described as a data structure that holds transactional records and while ensuring security, transparency, and decentralization. You can also think of it as a chain or records stored in the forms of blocks which are controlled by no single authority. A blockchain is a distributed ledger that is completely open to any and everyone on the network. Once an information is stored on a blockchain, it is extremely difficult to change or alter it. Blockchain and Cryptocurrency is vastly discussed now days in all research domains to bring the decentralization. This course is to understand Blockchain and its main application cryptocurrency.

Course Objectives:

- To build expertise in Blockchain and Distributed Ledger Technology
- To understanding basics of Cryptocurrency - Bitcoin
- To understanding Smart Contracts

Pre-requisite: Basics of Elliptic Curve Cryptography, Decentralized or Distributed Computing, Peer- to-peer Computing, Basic knowledge of programming.

Course Outcome: The students will be able to

· Get expertise in Blockchain and Distributed Ledger Technology
· Get Hands-on PoC experience across major Blockchain Platforms
· Exposure to Blockchain Use Cases across Domains

Pedagogy: Lecture delivery via discussions, whiteboard, slideshows, case studies' implementation

Contents:

UNIT I	7 hrs
Basics: Distributed Database, Two General Problem, Byzantine General problem And Fault Tolerance, Hadoop Distributed File System, Distributed Hash Table, ASIC resistance, Turing Complete. Cryptography: Hash function, Digital Signature - ECDSA, Memory Hard Algorithm, Zero Knowledge Proof.	
UNIT II	8 hrs
Blockchain: Introduction, Advantage over conventional distributed database, Blockchain Network, Mining Mechanism, Distributed Consensus, Merkle Patricia Tree, Gas Limit, Transactions and Fee, Anonymity, Reward, Chain Policy, Life of Blockchain application, Soft & Hard Fork, Private and Public blockchain	

UNIT III	8 hrs
Distributed Consensus: Nakamoto consensus, Proof of Work, Proof of Stake, Proof of Burn, Difficulty Level, Sybil Attack, Energy utilization and alternate. Cryptocurrency: History, Distributed Ledger, Bitcoin protocols - Mining strategy and rewards, Ethereum - Construction, DAO, Smart Contract, GHOST, Vulnerability, Attacks, Sidechain, Name coin	
UNIT IV	7 hrs
Cryptocurrency Regulation: Stakeholders, Roots of Bitcoin, Legal Aspects - Cryptocurrency Exchange, Black Market and Global Economy. Blockchain Applications: Internet of Things, Medical Record Management System, Domain Name Service and future of Blockchain	
Text books	
1. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, 2016.	
2. Wattenhofer, The Science of the Blockchain, 2016	
3. Josh Thompson, 'Blockchain: The Blockchain for Beginnings, Guild to Blockchain Technology and Blockchain Programming', Create Space Independent Publishing platform, 2017	
4. Chad Steel, "Windows Forensics", Wiley India, 2006	
5. Nelson, B, Phillips, A, Enfinger, F, Stuart, C., "Guide to Computer Forensics and Investigations, Thomson Course Technology, ISBN: 0-619-21706-5.	
Reference books	
1. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System	
2. Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli, A survey of attacks on Ethereum smart contracts	