Indira Gandhi Delhi Technical University for Women

(Established by Govt. of Delhi vide Act 09 of 2012)

Kashmere Gate, Delhi–110006

Scheme of Examination

&

Detailed Syllabus

(w.e.f. Academic Year 2021-2022 onwards)

for

Masters of Technology
(Information Technology-Cyber Security)

Department of Information Technology

PROGRAMME OUTCOMES

PO1. An understanding of the theoretical foundations and the limits of secure computing.
PO2. An ability to design, develop and evaluate new computer based systems for novel cyber security applications which meet the desired needs of industry and society.
PO3. Understanding and ability to use advanced cyber security techniques and tools.
PO4. An ability to undertake original research at the cutting edge of cyber security& its related areas.
PO5.To prepare graduates who will perform both as an individual and in a team through good analytical, design and implementation skills.

PO6. To prepare graduates who will be lifelong learners through continuous professional development.

PROGRAMME SPECIFIC OUTCOMES

PSO1.To develop students into an ethical Cyber Security Professional.
PSO2.To impart interdisciplinary technical knowledge & skills needed to protect computer systems from vulnerabilities, detect & respond to security breaches and cyber threats of all kinds
PSO3.To produce post graduates who can perform cyber security risk assessment, troubleshoot performance issues, offer information assurance which can be applied immediately in their workplace or research areas viz.

FIRST SEMESTER

S. No.	Subject 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		**22**	

SECOND SEMESTER

S. No.	Subject 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		**24**	

THIRD SEMESTER

Track-1

S. No.	Subject 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		**15**	

Track-2 Research Project

S. No.	Subject 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		**15**	

Track -3 Industry Project

S. No.	Subject 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		**15**	

FOURTH SEMESTER

S. No.	Subject Code	Subject	L-T-P	Credits	Category
1.	MIS-252	Dissertation – II/Project Work-II/Research Project Work-II	-	20	ROC
		Total		**20**	

List of Departmental Elective Courses

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

Advanced Programming	
Course Code: MIS-101 Contact Hours: L-3 T-0 P-2 Course Category: DCC	Credits: 4 Semester: 1

Introduction:

This course is designed to enable students to recognize the need for distributed, transactional and portable applications that leverage speed, security and reliability of server side technologies. This course shall inculcate programming capability to handle business logic and develop and deploy applications using Java Platform, Enterprise Edition.

Course Objectives:

- To Explore advanced topic of Java programming for solving problems
- Be able to put into use the advanced features of the Java language to build and compile web based applications
- To learn web service technology, hibernate framework
- Provide a strong foundation in tools, technology, and framework for students

Prerequisite:

Basic Knowledge of Object Oriented programming, Java Programming Language and Database Management

Course Outcomes: After studying this course student will be able to:

CO1: Understand concepts related to Java technology, build classes and reusable java programs using inheritance, polymorphism, interface and packages.

CO2: Demonstrate the use of multithreading, networking and web application framework and learn access to database through JDBC.

CO3: Implement electronic messages through java email and understand annotations, Hibernate Framework to apply in real world applications.

CO4: Implement web services application for transacting web applications built on varied Platforms and make effective use of tools

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 subject. The use of ICT and web-based sources will be adopted.

UNIT I:	**10 Hours**
Introduction to Java, Features of Java 8 and EE 8 , Variables, Arrays, Strings, Exception Handling, Multithreading, Collection Framework, Creating Interfaces, packages, JAR Files, Annotations , JDBC.Networking and Security Programming, socket Programming, Session Handling, Remote Method Invocation	
UNIT II :	**11 Hours**
Working with Servlets, Event Handling and Wrappers, Working with Java Beans, bean validation, Java Server Pages, Expression Languages, JSP Application Development, Tags Extensions and Implementation JSP Tag Library, Implementing Filters.	
UNIT III :	**10 Hours**
Working with java Server Faces, Understanding Java Mail, Java EE Design Patterns, Working with Hibernate, Struts, Spring MVC, Spring configuration. Case Study such as (Any One): Building an Online Book Store, Online Shopping cart, University Management System , simple e-commerce application - Forest case Study	
UNIT IV :	**11 Hours**
Implement SOA using Java Web Services, JSON Processing, Building Web services with JAX, Building SOAP , UDDI, RESTFul services, Working with Glassfish, JBOSS server, JUnit Testing Security in JAVA EE.	
Text Books	
1. Jim Koegh, “Java EE Complete Reference”, Mc Graw Hill , First Edition, 2017	
2. “Core and Advanced Java, Black Book”, DreamTech Publications, First Edition, 2018.	
3. Java Platform, Enterprise Edition 8: The Java EE Tutorial, Oracle, Java Documentation, 2018.	
Reference Books	
1. David R. Heffelfinger, “Java EE 8 Application Development”, Packt Publishing, First Edition, December 2017	

Advances in Machine Learning	
Course Code: MIS-103 Contact Hours: L-3 T-0 P-2 Course Category: DCC	Credits: 4 Semester: 1

Introduction:
Machine learning is the science of getting computers to act without being explicitly programmed. Many researchers also think it is the best way to make progress towards human-level AI. This course provides a broad introduction to machine learning, data mining, and statistical pattern recognition.

Course Objectives:
- To provide an introduction to the basic principles, techniques, and applications of Machine Learning.
- To explain the strengths and weaknesses of different machine learning algorithms (relative to the characteristics of the application domain)
- To be able to adapt or combine some of the key elements of existing machine learning algorithms to design new algorithms as needed.

Prerequisite: Knowledge of Programming, Discrete Mathematics (Set Theory, Graph Theory, Logic), Basic Probability Theory and Statistics, and Data Structures and Algorithms

Course Outcomes: After studying this course students will be able to:
CO1: Gain a broad understanding of the machine learning process.

CO2: Analyze different classification algorithms.

CO3: Understand unsupervised learning.

CO4: Understand advanced algorithms in machine learning.

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 subject. The use of ICT and web-based sources will be adopted.

UNIT I:	12 Hours
Introduction to Machine Learning, Well Posed Problems, Machine Learning Process, Designing a Learning System, Types of Machine Learning, Application of Machine Learning, Prospectives and Issues In Machine Learning. Features, Feature Vectors, Feature Selection And Visualization, Testing ML Algorithms (Overfitting, Training, Testing, And Validation Sets, Confusion Matrix, Accuracy Metrics, ROC Curve, Unbalanced Datasets, Measurement Precision), Turning Data into Probabilities (The Naïve Bayes' Classifier), Some Basic Statistics. The Brain And The Neuron, Neural Networks, The Perceptron, Linear Separability And Regression (Linear And Logistic Regression) , The Multi-Layer Perceptron, Forward And Back-error propagation, Radial Basis Functions And Splines. The Curse Of Dimensionality, Dimensionality Reduction, Principle Component Analysis, Linear Discriminant Analysis (LDA), Factor Analysis, Independent Components Analysis (ICA).	
UNIT II :	**10 Hours**
Probabilistic Learning, Gaussian Mixture Models, Nearest Neighbor Methods. Support Vector Machines-Optimal Separation, Kernels, Svm Algorithm And Extension. Learning With Decision Tree, ID3, CART, Ensembling Learning, Boosting, Bagging, Random Forest. Different Ways To Combine Classifiers. Optimization And Search Techniques – Going Downhill, Least-Squares Optimisation, Search Approaches (Exhaustive Search, Greedy Search, Hill Climbing).	
UNIT III :	**9 Hours**
Evolutionary Learning, Genetic Algorithm, GENERATING OFFSPRING, GENETIC PROGRAMMING, Particle Swam Optimization. Unsupervised Learning, Clustering, Mixture Models, K-Means Clustering, Hierarchical Clustering, Distributional Clustering, Self-Organising Map (SOM). Evaluation Parameters For Unsupervised Learning. Reinforcement Learning: State And Action Spaces, Action, Policy, Markov Decision Processes, The Difference Between SARSA And Q-Learning, Uses Of Reinforcement Learning	
UNIT IV :	**11 Hours**
Markov Chain Monte Carlo (MCMC) Methods, Graphical Models, Bayesian Networks, Hidden Markov Models (HMMS), Tracking Methods.Advance Machine Learning Techniques - Gaussian Process Regression, Energetic Learning: The Hopfield Network, The Boltzmann Machine, Restricted Boltzmann Machine (RBM) Deep Learning- Deep Belief Networks(DBN), Convolution Neural Networks (CNN).	
Text Books	
1. Chapman & Hall, Machine Learning: An Algorithmic Perspective, CRCF Press, Second Edition, 2015	
2. Christopher Bishop, Pattern Recognition and Machine Learning, Springer, 2nd Edition, 2010	
3. Tom Mitchell, Machine Learning, McGraw Hill, 2017	
Reference Books	
1. T. Hastie, R. Tibshirani, J. Friedman. The Elements of Statistical Learning, 2e, 2008.	
2. Han, Jiawei, Jian Pei, and Micheline Kamber, Data Mining: Concepts and Techniques, Elsevier,2011	

Advanced Data Structures and Algorithms	
Course Code:MCS-105 Contact Hours: L-3 T-0 P-2 Course Category: DCC	Credits: 4 Semester: 1

Introduction:

This course builds upon the introductory courses in data structures. It introduces students to a number of highly efficient data structures for solving data driven computational problems across a variety of areas.

Course Objectives:

- To impart knowledge of computational and advanced concepts of Data structures and algorithms.
- To understand concepts about searching algorithms, lists, graphs and trees.
- To understand about writing algorithms and sequential approach in solving problems with advanced Data structures

Prerequisite: Knowledge of fundamentals of Data Structures, Algorithms and Analysis.

Course Outcomes: After studying this course students will be able to:

CO1: Define advanced highly efficient data structures and their properties.

CO2: Understand the concept of space and time complexity and compare the efficiency of algorithms.

CO3: Apply the advanced highly efficient data structures to solve computational problems.

CO4: Design and employ network flow algorithms to 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.

UNIT I:	10 Hours
Review of data structures: Arrays, Stacks, Linked Lists, Queues. Hash tables – collision resolution, Hash functions, Open addressing. Dictionary. Data Frames and operations. Multi-dimensional Arrays (NumPy) and operations.	
UNIT II :	**10 Hours**
Binary trees and their properties, threaded binary trees - differentiation, leftist trees, tournament trees, use of winner trees in merge sort as an external sorting algorithm, bin packing, Binary search trees, search efficiency, insertion and deletion operations, importance of balancing, AVL trees, searching, insertion and deletions in AVL trees, Tries, 2-3 tree, B-tree	
UNIT III :	**10 Hours**
Review of Graphs – DFS and BFS, MST, Shortest Path – Single Source and All Pair. Degree Distribution, Paths, Distances, Connectedness, Clustering Coefficient, Random Networks – Evolution, Small World, Barabasi-Albert Model.	
UNIT IV :	**10 Hours**
Network Flow: Max-Flow problem, Ford-Fulkerson algorithm, Augmenting paths, Bipartite Matching problem, Applications: Airline Scheduling, Image Segmentation. Evolving Networks: Bianconi-Barabasi Model.	
Text Books	
1. A. Aho, J. Ullman, J. Hopcroft.,"Data Structures and Algorithms", Pearson Education India, 1st Edition, 2002/Latest edition	
2. J. Kleinberg and E. Tardos. "Algorithm Design", Pearson Publication, 1st Edition, 2005/Latest edition	
Reference Books	
1. T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, "Introduction to Algorithms", MIT Press, 3rd Edition, 2009/Latest edition.	
2. Al. Barabasi. "Network Science", Cambridge University Press, 2016/Latest edition.	
3. P. Brass, "Advanced Data Structures", Cambridge University Press, 1st Edition, 2008/Latest edition	
4. T. Cormen, C. Leiserson, R Rivest, C. Stein, "Introduction to Algorithms", MIT Press, 3rd Edition, 2009/Latest edition.	

Fundamentals of Information Security	
Course Code:MIS-105 Contact Hours: L-3 T-1 P-2 Course Category: DCC	Credits: 4 Semester: 1

Introduction:

This course will introduce students to fundamentals of information security, cryptography, access control mechanisms, system attacks and defences against them

Course Objectives:

- Identify the basic security issues in the computer network communications.
- Understand the concept of Cyber security and issues and challenges associated with it.
- Analyze the vulnerabilities in any computing system and hence be able to design a security solution
- Evaluate various security mechanisms used in real world

Course Outcomes: After studying this course students will be able to:

CO1: To understand the basic concept of Information Security and their mathematical models, encrypt and decrypt messages using block ciphers and public key cryptosystems.

CO2: To identify well-known signature generation and verification algorithms and apply them to sign and authenticate messages.

CO3: To identify and classify computer and security threats and develop a security model to prevent, detect and recover from attacks.

CO4: To use and apply various security mechanisms to solve real world problems

Pedagogy: The teaching-learning of the course would be organized through lectures, assignments, case studies/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 sources as well as flipped class room teaching will be adopted.

UNIT I:	**10 Hours**
Security Overview, CIA model, Threats, Policy and Mechanisms, Security Policies, Confidentiality Policies, Integrity Policies, Hybrid Policies, Cryptography Basics, Classical Cryptosystems, Stream Ciphers and Block Ciphers, Public Key Cryptography: RSA.	
UNIT II :	**11 Hours**
Cryptographic Checksums , Authentication Basics, Password management, Challenge Response, Biometrics, Key Exchange, Certificate Chains, X.509, Digital Signatures, Access Control Lists: Creation and Maintenance, Revocation of Rights, Ring based Access Control.	
UNIT III :	**11 Hours**
Malicious Logic, Trojan Horses, Viruses, Worms, Logic Bombs, Defenses, Sandboxing, Intrusion Detection: Principles and Basics, Anomaly modelling, Architecture: Host and network based Information Gathering, Organization of Intrusion Detection Systems, Intrusion Response.	
UNIT IV :	**10 Hours**
Firewalls and Proxies, DMZ server, User Security: Policy, Access, Files and Devices, Processes, Electronic Communications, Program Security: Requirements and Policy, Design, common security related programming problems, Virtual Machines Structure.	
Text Books	
1. Matt Bishop, S.S. Venkatramanayya, “Introduction to Computer Security, 3/e”, Pearson Education	
2. W Stallings, “Cryptography and Network Security: Principles and Practice, 6/e”, Prentice Hall	
Reference Books	
1. B. Forouzan, D. Mukhopadhyay, "Cryptography and Network Security 2/e", Tata-McGraw Hill	

General Open Elective -1	
Course Code:GEC-101 Contact Hours: L-T-P 2-0-0/ 1-1-0 / 0-0-4 Course Category: GEC	Credits: 2 Semester: 1

Introduction:

A Generic Elective (GE) course is an inter-disciplinary course provided to the students ,chosen generally from an unrelated discipline/subject and allowing them a chance at comprehensive education. GEs are introduced as part of the CBCS. The students can choose their preference from a pool of courses from various disciplines/subjects.Elective courses do much more than filling in the gaps to fulfill the high school graduation requirements. It gives a chance to explore new options, allowing students to study more about the subject they are passionate about, and enables them to 'test drive' new activities. They provide students with the necessary skills to improve creativity that they might not find in the classroom. The main purpose of the elective course is to seek exposure to a new discipline/subject and to provide the students with an alternative option for desired fields.

Course Objectives:

- Students will have exposure to a new discipline/subject.
- Prepare students to look for inter-disciplinary research.
- Fulfill the limitation to pursue master's study in desired field.
- Help discover new things that never existed and might change the course of student's life.

Prerequisite: Basic knowledge of the selected domain of elective course

Course Outcomes: After studying this course students will be able to:

CO1: Identify new discipline and learn new subject for future careers.

CO2: Apply their knowledge to understand and solve the real life problems.

CO3: Analyse creative design process through the integration and application of diverse technical knowledge and expertise to address social issues.

CO4: Develop the habit of working independently to attain self-motivation, discipline, and confidence to achieve their goals.

Pedagogy: The teaching-learning of the course would be organized through lectures, assignments, case studies/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 sources as well as flipped class room teaching will be adopted.

Cyber Security and Forensics	
Course Code: MIS-107 Contact Hours: L-3 T-0 P-2 Course Category: DEC	Credits: 4 Semester: 1

Introduction:

Cyber Security and Forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. This course provides for a broad introduction of cyber security and forensics concepts, industry best practices for information security and key security concepts that will protect an organization against fraud, data breaches and other vulnerabilities. It enables the students to gain in-depth knowledge in the field of Computer forensics & Cyber Crime.

Course Objectives:

- To maintain an appropriate level of awareness, knowledge and skill to allow students to minimize the occurrence and severity of information security incidents.
- To learn techniques used to detect, respond and prevent network intrusions.
- To identify and apply appropriate forensics tools to acquire, preserve and analyze system image.
- To protect information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability.
- Identify sources of evidentiary value in various evidence sources including network logs, network traffic, volatile data.

Prerequisite: Knowledge of Computer Networking, Linux, UNIX, Understanding of Web Application Architecture and HTTP/HTTPS communication.

Course Outcomes: After studying this course students will be able to:

CO1: Understand the fundamentals of Cyber Security and comprehend the incident response process.

CO2: Demonstrate the difference between data acquisition techniques.

CO3: Apply forensic analysis tools to recover important evidence for identifying cyber-crime.

CO4: Apply investigation tools and techniques for analysis of data to identify evidence related to cyber-crime and use available digital forensics tools.

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. Course will have a blend of theory and practice for the benefit of students. Use of ICT, web based sources as well as blackboard teaching will be adopted.

UNIT I:	**12 Hours**
Cyber Security Concepts, Security Goals, Security Services, Types of Cybercrime, Cyber Attack Process, Introduction to Incident Response Process, Computer Security Incident, Goals of Incident response, Who is involved in Incident response, Incidence Response Methodology, Pre Incident preparation, Detection of Incidents, Initial response, Formulate a response strategy, Investigate the incident, Reporting and Resolution.	
UNIT II :	**10 Hours**
Computer Forensics Fundamentals, Data Acquisition of digital evidence from electronic media, Acquisition tools, Evidence collection and preservation, Windows Forensics, Live data collection from Windows systems, Live data Collection from Unix systems.	
UNIT III :	**10 Hours**
Sources of Digital/Electronic Evidence, Computer Forensic Analysis and Validating Forensics Data, System Forensics, Network Forensics, Database Forensics, Fighting against Macro Threats, Information Warfare Arsenal, Tactics of the Military	
UNIT IV :	**10 Hours**
Malware forensics, Mobile Device Forensics, Google Forensics, Internet Forensics, Email Forensics, Messenger Analysis, Web Forensics, Current Computer Forensics Tools: Software/Hardware Tools. An Indian perspective on digital forensics: Indian IT act, Cyber laws.	
Text Books	
1. K Mandla, C. Prosise , Matt Pepe, " Incident Response and Computer Forensics", McGraw Hill, 2nd Edition, 2003	
2. Chad Steel, "Windows Forensics", Wiley India, 1st Edition, 2006	
3. Nelson, B, Phillips, A, Enfinger, F, Stuart, C., "Guide to Computer Forensics and Investigations, Thomson Course Technology, 4th Edition, 2009	
Reference Books	
1. Keith J. Jones, Richard Bejtiich, Curtis W. Rose, Real Digital Forensics, Pearson Education, 1st Edition, 2005	
2. Computer Forensics, Computer Crime Investigation by John R. Vacca, Firewall Media, New Delhi	

Digital Identity and Access Management	
Course Code: MIS-109 Contact Hours: L-3 T-0 P-2 Course Category: DEC	Credits: 4 Semester: 1

Introduction:

The course aims to familiarize the students with the advanced concepts of Digital Identity in cyber space and Enterprise Access Management Frameworks. Identity and access management (IAM) enables the right individuals to access the right resources at the right times for the correct reasons. IAM addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet increasingly rigorous compliance requirements. The course is designed for inculcating the research aptitude in graduate students, keeping the needs of Enterprise Security and Privacy in Industry 4.0.

Course Objectives:

- To comprehend importance of Digital Identity in Cyber Space in Industry 4.0
- To learn the Identity and Access Management Framework
- To understand Privileged Access Management Life Cycle Management and Provisioning
- To identify Security and Privacy Issues in an Enterprise Access Management Framework

Prerequisite: Basic understanding of Cyber Space and Web Technologies, Internet Security, Pseudo-randomness, Cryptography, Security and Privacy Issues in Industry 4.0

Course Outcomes: Upon Successful completion the students will be able to:

CO1: Understand the basic concepts of Identity Management and Authentication Systems.

CO2: Develop Access control mechanism in cloud environment.

CO3: Analyze the Access validation and certification, Segregation of Duties and System for Cross-domain Identity Management.

CO4: Apply the concepts of Intellectual Property and laws and regulations of Industry for digital security.

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.

UNIT I:	10 Hours
Introduction - IAAA: Identity Management – Terms & Concepts, Identity Management – Players & Actors, CIA Principles, Cyber Security-Privacy and Trust, Kerberos, IAAA (Identification, Authentication, Authorization and Accounting) Operation, Identity & Authentication Assurance Levels, Digital Identity Framework and SSO, Identity Federation – Evolution & Concepts, IdentityFederation Standards – SAML & OAuth, Web Services Federation and OAuth, Authentication Factors, Biometrics. **Authentication Systems:** Role of Certificates and PKI in Authentication, PKI, Smart Cards & Authentication Systems, Overview of Authentication Systems, Role of Biometrics	
UNIT II :	**10 Hours**
Access Control: Access Control Concepts, Introduction to Access Control Structures, Access control Policies & Models, Identity & Access Control in Cloud Environments, RBAC and ABAC, Identity & Access Control in Cloud Environments, Privacy, PII & Privacy Policies. **Privileged Account Management (PAM):** Privileged Access Management, Privileged Accounts, Privileged Account and Session Management, Privileged Account Monitoring, Privileged Account Management Solutions, Application Whitelisting	
UNIT III :	**10 Hours**
Identity Governance and Administration: User Onboarding, User Termination & Role changes, Access Controls & RBAC, Information Security Access Controls, Centralized, Decentralized, and Role based access controls, Access validation & Certification, Segregation of Duties, Auditing and Reporting, Identity Lifecycle Management, System for Cross-domain Identity Management.	
UNIT IV :	**10 Hours**
Data Governance and Protection: Data Types, Intellectual property, Data Classification, Industry and local laws and regulations, Data Type Management & Monitoring, Security Policy Framework, Data Breach and Incident Response Process, Notifiable Data Breaches	
Text Books	
1. Ertem Osmanoglu, "Identity and Access Management: Business Through Connected Intelligence", Elsevier Science, Syngress, November 2013	
2. Omondi Orondo, "Identity and Access Management: A Systems Engineering Approach", IAM Imprints 1st edition, 2014	
3. Graham Williamson, David Yip, and Ilan Sharoni, "Identity Management: A Primer", MC Press, September 2009	
Reference Books	
1. Michael E. Whitman and Herbert J. Mattord, "Management of Information Technology", Cengage Learning 4th Edition, 2013	
2. Elisa Bertino and Kenji Takahashi, "Identity Management: Concepts, Technologies and Systems", Artech House, 2011	

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 Objectives:

- 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.

Prerequisite: Basic Knowledge of Programming Language (s), Database Management, Network, Server.

Course Outcomes: Upon Successful completion the students will be able to:

CO1: Acquire security requirements with respect to software development.

CO2: Design and implement software development with minimum software vulnerabilities

CO3: Write and test software code with respect to security testing and remove security flaws.

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.

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 :	**12 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++ (2^{nd} 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

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 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 Objective:

- To understand the fundamentals of Cryptography
- To acquire knowledge on standard algorithms used to provide confidentiality, integrity and authenticity
- To explain and use modern cryptographic methods (symmetric encryption, public key encryption, hash functions, key management, digital signatures, certificates)
- To discuss electronic mail security, SSL/TLS and recent developments affecting security and privacy on the Internet.

Pre-requisite: None

Course Outcome:

CO1: Understand applied cryptographic basics.

CO2: Analyze and differentiate between public-key and private key cryptosystems.

CO3: Evaluate security mechanisms using rigorous approaches by key ciphers and hash functions.

CO4: Design cryptographic protocols to 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.

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 :	**12 Hours**
Asymmetric Cryptography: Number Theory, public key cryptography: RSA, ElGamal, and Elliptic Curve Cryptography, Diffie Hellman Key management , Digital Certificates: X.509	
UNIT III :	**12 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 Objectives:

- 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

Prerequisite: Nil

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

CO1: Understand the basics of Linear Algebra and Matrix Decomposition.

CO2: Apply the concept of Vector calculus and Linear Algebra for solving Regression problems.

CO3: Evaluate the density estimation problems using Probability and Distributions.

CO4: Develop Optimization techniques to solve the classification 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 class room teaching will be adopted.

UNIT I:	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 II :	**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 III :	**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 IV :	**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	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 organizations 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

Prerequisite: Cyber Security Fundamentals.

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

CO1: Understand Cyber security risk management framework and methodologies.

CO2: Analyse the information security risks.

CO3: Design the cyber risk mitigation model.

CO4: Plan and articulate 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.

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

Prerequisite: Fundamentals of Information Security

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

CO1: Understand applied cryptographic basics and its applications.

CO2: Analyze 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.

CO3: Develop interactive protocols that allow the signer to prove a forgery and limit who can verify the signature.

CO4: Apply the right algorithm, protocol, and systems to develop secure systems to protect digital assets in the cyber world.

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.

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.

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 Objectives:
- 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.

Prerequisite: Programming, Machine learning.

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

CO1: Understand the concepts of machine learning and its requirement in cyber systems from a security perspective.

CO2: Analyze pattern for malware detection and authentication in mobile security.

CO3: Develop a mechanism to detect Email spam, malicious URLs and phishing attack.

CO4: 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.

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 :	**11 Hours**
Behavioral Biometrics: Keyboard & Mouse Pattern Analysis, Active authentication. **Mobile Security:** Static & Dynamic Analysis, Malware Detection.	
UNIT III :	**11 Hours**
W**eb 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

Prerequisite: Computer Networks.

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

CO1: Illustrate reference models with layers, protocols and interfaces. Summarize functionalities of different Layers.

CO2: Combine and distinguish functionalities of different Layers. Describe and Analysis of advanced protocols of computer networks, and how they can be used to assist in network design and implementation.

CO3: Understand principles behind the latest advances in advanced network technology

CO4: Develop the understanding of Content and Wireless Networks and various network security mechanisms

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.

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 Ad Hoc 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 Network , 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 FireWall , Radio Networks , Opportunistics Network.	
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	
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	

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-requisites: Cyber Security Fundamentals

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

CO1: Describe the fundamentals of cyber world and cyber law in general and technicalities of law in cyber world.

CO2: Interpret issues relating to regulation and explain various facets of cyber-crimes; and use different plagiarism tool.

CO3: Comprehend the Intellectual Property issues and E-Commerce in the cyber space.

CO4: Distinguish between different laws and regulations in cyber space at national and international level.

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.

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 :	**12 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 :	**12 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.

Prerequisite: Knowledge of object oriented programming principles, Basic understanding of Machine Learning.

Course Outcomes: Upon Successful completion the students will be able to:

CO1: Understand security and privacy challenges in any social media platform

CO2: 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

UNIT I:	10 Hours
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	
UNIT II:	**11 Hours**
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	
UNIT III:	**11 Hours**
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.	
UNIT IV:	**10 Hours**
Social Media Case Studies - Facebook, Twitter, Instagram, YouTube, LinkedIn, StackOverflow, GitHub, Quora, SnapChat, Reddit, FourSquare, Yelp..	
Text Books	
1. Zafarani, Reza, Mohammad Ali Abbasi, and Huan Liu. Social media mining: anintroduction. Cambridge University Press, 2014.	
Reference Books	
1.Bonzanini Marco. Mastering Social Media Mining. Packt Publishing, 2016	
2. Mikhail Klassen, Matthew A. Russell. Mining the Social Web. 3rd Edition. O'Reilly Media, Inc, 2019	

Research Methodology and Publication Ethics	
Course Code: ROC-902 Contact Hours: L-3 T-1 P-0 Course Category: ROC	Credits: 4 Semester: 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. programming.

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: Upon Successful completion the students will be able to:

CO1: Gain knowledge and comprehend various fundamentals of research.Build a sound foundation of methodologies and applications of research.

CO2: Identify and analyze relationship between technical/multidisciplinary areas and integrate them for various applications.

CO3: Evaluate and apply the quantitative and qualitative aspects of research to innovate devices and processes in the constantly competitive Technologies.

CO4: Identify and evaluate the Cross functional coalition aspects, know how on how to take research to a product implementation

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.

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..	
Text 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: Fundamentals of Information Security (MIS-105)

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

CO1: Understand aspects of security, importance of data gathering, foot printing and system hacking.

CO2 : Compare and analyze advanced concepts such as DDoS Attacks, Buffer Overflows, SQL Injection, Cross Site Scripting, Virus Creation

CO 3: Analyze and test ethical hacking tools and techniques

CO 4: Develop technical skills with in-depth knowledge of ethical hacking concepts that will assist them to take certification exam in future

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.

UNIT I:	10 Hours
Introduction to Ethical Hacking, Hacking Laws, Foot-printing, Reconnaissance, Google hacking, Vulnerable sites, Using Google as a Proxy Server, Directory Listings, Locating Directory Listings, Finding Specific Directories, Finding Specific Files, Server Versioning, Scanning, System hacking Cycle, Enumeration, Cracking Password, Types of password attacks	
UNIT II :	**11 Hours**
Trojans and Backdoors, Types of Trojans, Viruses, Worms, 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 :	**11 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, Hacking web servers, Web Server Defacement, Proxy and Packet filtering, SQL Injection, Cross Site Scripting	
UNIT IV :	**10 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: HTTP, Basic, Digest, NTLM, Negotiate, Certificate based, Forms-bases, 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.

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

Course Outcomes: Upon Successful completion the students will be able to:

CO1: Conceptual clarity in Grid and Cloud Computing architecture.

CO2: Conceptual understanding of Virtualization at different levels

CO3: Logical insight for comprehending the Security Primitives in Cloud Computing.

CO4: 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.

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 Contact Hours: L-2 T-0 P-2 Course Category: DEC	Credits: 3 Semester: 3

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 mean that 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.

Prerequisite: Basic Knowledge of Software applications, programming, Database, Network Concepts.

Course Outcomes: Upon Successful completion the students will be able to:

CO1: Learn what to test, which modules to test and how to test for software security issues.

CO2: Perform Security testing of software and web applications

CO3: Detect Security vulnerabilities in software and network.

CO4: Implement Security patterns and security controls to secure Software applications and network.

CO 5: Assess, evaluate and analyze risk of a software applications using standard Risk assessment and Management Framework.

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.

UNIT I:	**8 Hours**
Introduction: Testing Objectives, Process, Principles, Tester Role in Software Development Organization, Test Case Implementation and Execution. Testing Concepts: Levels of Testing, Test Cases Design and Strategy, Test Suite, 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 :	**8 Hours**
Software Vulnerabilities fundamentals: causes of software vulnerabilities, principle and Classification of software vulnerabilities, authentication and authorization, classification of SQL Injection attacks, buffer overflow, distributed denial of service attacks, , session attacks, Cross site scripting, Cross site request forgery (CSRF), Format string problems, Integer overflows.	
UNIT III :	**7 Hours**
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 :	**7 Hours**
Risk Management, Categories of Risk, Approaches to Risk Identification, Analyzing Risk, Qualitative Analysis and quantitative analysis, conducting Routine security review, Working with management, Responding to Security Incidents, ranking the risk associated with a vulnerability, Vulnerability scoring system CVSS, VRSS, Risk Prioritization, Planning the risk response, Updating Security Policy, Taxonomy of information security risk assessment. Case Study : Risk Assessment and Management Framework (NIST, OCTAVE-Allegro, OCTAVE-S)	
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:

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 mean that 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 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

Prerequisite: Proficiency in at least one programming language.

Course Outcomes: Successful completion the students will be able to:

CO1: Identify and discuss the characteristics of different NLP techniques.

CO2: Identify and discuss the characteristics of machine learning techniques used in NLP.

CO3: Implement a hidden Markov model for part-of-speech tagging

CO4: 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).

CO 5: 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

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**
nformation 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

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/106/106/106106211/
4. https://nptel.ac.in/courses/106/105/106105158/

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

CO1: Understand working knowledge of deep architectures used for solving various Vision and NLP tasks.

CO2: Analyse the deep learning algorithms which are more appropriate for various types of learning tasks in various domains.

CO3: Develop deep learning techniques such as Convolutional Neural Network and Recurrent Neural Network for malware detection.

CO4: Apply deep learning techniques such as Restricted Boltzmann and Markov Chains for malware detection using text processing.

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.

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	
2. Natural Language Process…ing and Information Retrieval: Tanvier Siddiqui, U.S. Tiwary, Oxford University Press,2008/Latest Edition	
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: L-2 T-0 P-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 Outcomes: Upon Successful completion the students will be able to:

CO1: Get expertise in Blockchain and Distributed Ledger Technology.

CO2: Get Hands-on PoC experience across major Blockchain Platforms

CO3: Exposure to Blockchain Use Cases across Domains

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.

UNIT I:	**7 Hours**
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 Hours**
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 Hours**
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 Hours**
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	

General Elective Course - II	
Course Code: GEC-201 Contact Hours: L-T-P 2-0-0/ 1-1-0 / 0-0-4 Course Category: GEC	Credits: 2 Semester: 3

Introduction:

A Generic Elective (GE) course is an inter-disciplinary course provided to the students chosen generally from an unrelated discipline/subject and allowing them a chance at comprehensive education. GEs are introduced as part of the CBCS. The students can choose their preference from a pool of courses from various disciplines/subjects. Elective courses do much more than filling in the gaps to fulfill the high school graduation requirements. It gives a chance to explore new options, allowing students to study more about the subject they are passionate about, and enables them to 'test drive' new activities. They provide students with the necessary skills to improve creativity that they might not find in the classroom. The main purpose of the elective course is to seek exposure to a new discipline/subject and to provide the students with an alternative option for desired fields.

Course objectives:

- Students will have exposure to a new discipline/subject.
- Prepare students to look for inter-disciplinary research.
- Fulfill the limitation to pursue master's study in desired field.
- Help discover new things that never existed and might change the course of student's life.

Prerequisite: Basic knowledge of the selected domain of elective course

Course Outcomes: After completion of the elective course, the students will be able to:

CO1: Identify new discipline and learn new subject for future careers.

CO2: Apply their knowledge to understand and solve the real life problems.

CO3: Analyse creative design process through the integration and application of diverse technical knowledge and expertise to address social issues.

CO4: Develop the habit of working independently to attain self-motivation, discipline, and confidence to achieve their goals.

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

Dissertation - I / Project Work	
Course Code: MIS - 251 Course Category: ROC	Credits: 8 Semester: 3

Course Outcomes:

CO1: Understand basic concepts in a specific domain of study.

CO2: Implement and Analyze the concepts in a specific domain of study.

CO3: Apply the concepts in a specific domain of study to solve a problem.

Industrial Training/Internship	
Course Code: MCA-253 Course Category: ROC	Credits: 1 Semester: 3

Course Objectives:

Students will carry on the industrial training/internship for at least six weeks in the summer break of previous academic session. The idea of the training is to make them capable of handling the implementation of their theoretical knowledge in the practical field. To facilitate the development of a holistic perspective among students towards life, industry experts teach advanced technologies. Through Industrial training, students get familiarize with the environment of an organization and a company. Students get a certificate which validates their skills and helps them in getting a job quickly. The assessment for the same will be done within the first two weeks of opening of academic session by the respective department.

Course Outcomes:

CO1: Understand the Organizational Structure of a company.

CO2: Develop work habits and attitudes necessary for job success (technical competence, professional attitude, organization skills etc.)

CO3: Develop written communication and technical report writing skills.

CO4: Develop an awareness for the need and applications of standards in the industry.

General Elective Course -II	
Course Code: GEC-201 Contact Hours: L-T-P 2-0-0/ 1-1-0 / 0-0-4 Course Category: GEC	Credits: 2 Semester: 3

Introduction:

A Generic Elective (GE) course is an inter-disciplinary course provided to the students chosen generally from an unrelated discipline/subject and allowing them a chance at comprehensive education. GEs are introduced as part of the CBCS. The students can choose their preference from a pool of courses from various disciplines/subjects. Elective courses do much more than filling in the gaps to fulfill the high school graduation requirements. It gives a chance to explore new options, allowing students to study more about the subject they are passionate about, and enables them to 'test drive' new activities. They provide students with the necessary skills to improve creativity that they might not find in the classroom. The main purpose of the elective course is to seek exposure to a new discipline/subject and to provide the students with an alternative option for desired fields.

Course objectives:

- Students will have exposure to a new discipline/subject.
- Prepare students to look for inter-disciplinary research.
- Fulfill the limitation to pursue master's study in desired field.
- Help discover new things that never existed and might change the course of student's life.

Prerequisite: Basic knowledge of the selected domain of elective course

Course Outcomes: After completion of the elective course, the students will be able to:
CO1: Identify new discipline and learn new subject for future careers.

CO2: Apply their knowledge to understand and solve the real life problems.

CO3: Analyse creative design process through the integration and application of diverse technical knowledge and expertise to address social issues.

CO4: Develop the habit of working independently to attain self-motivation, discipline, and confidence to achieve their goals.

Industrial Training/Internship	
Course Code: MIS 253 Course Category: ROC	Credits: 1 Semester: 3

Course Objectives:

Students will carry on the industrial training/internship for at least six weeks in the summer break of previous academic session. The idea of the training is to make them capable of handling the implementation of their theoretical knowledge in the practical field. To facilitate the development of a holistic perspective among students towards life, industry experts teach advanced technologies. Through Industrial training, students get familiarize with the environment of an organization and a company. Students get a certificate which validates their skills and helps them in getting a job quickly. The assessment for the same will be done within the first two weeks of opening of academic session by the respective department.

Course Outcomes:

CO1: Understand the Organizational Structure of a company.

CO2: Develop work habits and attitudes necessary for job success (technical competence, professional attitude, organization skills etc.)

CO3: Develop written communication and technical report writing skills.

CO4: Develop an awareness for the need and applications of standards in the industry.

Dissertation - II / Project Work	
Course Code: MIS - 252 Course Category: ROC	Credits: 20 Semester: 4

Course Outcomes:

CO1: Understand basic concepts in a specific domain of study.

CO2: Implement and Analyze the concepts in a specific domain of study.

CO3: Apply the concepts in a specific domain of study to solve a problem.