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 2019-2020 onwards)

For

Masters of Technology

(Information Technology – Information Security Management)

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.	Code	Subject	L-T-P	Credits	Category
1.	MIS-101	Advanced Programming	3-0-2	4	DCC
2.	MIS-103	Secure Coding and Security Engineering	3-0-2	4	DCC
3.	MIS-105	Fundamentals of Information Security	3-0-2	4	DCC
4.	MCS-107	Data Structures and Algorithm Analysis	3-0-2	4	DCC
5	GEC-101	Generic Open Elective	2-0-0 1-1-0 0-0-4 0-2-0	2	GEC
6.	ROC-101	Research Methodology	3-0-0	3	ROC
		Total		21	

SECOND SEMESTER

S. No.	Code	Subject	L-T-P	Credits	Category
1.	MIS-102	Advances in Machine Learning	3-0-2	4	DCC
2.	MIS-104	Applied Cryptography	3-1-0	4	DCC
3.	MIS-106	Cyber Security and Forensics	3-0-2	4	DCC
4.	DEC-1xx	Departmental Elective Course – 1	3-0-2 3-1-0 2-1-2	4	DEC
5.	DEC-1xx	Departmental Elective Course – 2	3-0-2 3-1-0 2-1-2	4	DEC
6	ROC-102	Research Ethics	3-0-0	3	ROC
		Total		23	

THIRD SEMESTER

S. No.	Code	Subject	L-T-P	Credits	Category
1.	MIS-201	Ethical Hacking	3-0-2	4	DCC
2.	DEC-2xx	Departmental Elective-3	3-0-2 3-1-0 2-1-2	4	DEC
3.	DEC-2xx	Departmental Elective-4	3-0-2 3-1-0 2-1-2	4	DEC
4	GEC-201	General Open Elective	2-0-0 1-1-0 0-0-4	2	GEC
5	MIS-251	Dissertation – I/Project Work	-	8	DCC
6	MIS-253	Industrial Training/Internship	-	1	DCC
		Total		23	

FOURTH SEMESTER

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

List of Departmental Elective Courses

Category	Course Code	Subject	Credits
Departmental Elective Course-1	MIS-108	Adv. Database Management Systems	3-0-2
	MIS-110	Introduction to Biometrics	3-0-2
	MIS-112	Computer Vision	3-0-2
	MIS-114	Blockchain Fundamentals	3-0-2
Departmental Elective Course-2	MIS-116	Soft Computing	3-0-2
	MIS-118	Semantic Web	3-1-0
	MIS-120	Security Testing and Risk Management	3-0-2
	MIS-122	Natural Language Processing and Information Retrieval	3-0-2
Departmental Elective Course-3	MIS-203	Neural Network and Deep Learning	3-0-2
	MIS-205	Security Patterns	3-0-2
	MIS-207	Cryptographic Protocols and Algorithms	3-0-2
	MIS-209	Advanced Network Technology	3-0-2
Departmental Elective Course-4	MIS-211	Cyber Laws and Rights	3-1-0
	MIS-213	Security and Privacy in Social Networks	3-1-0
	MIS-215	Software Defined Networks	3-1-0
	MIS-217	Cloud Computing Architecture and Security	3-0-2

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:

- 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:

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

Secure Coding and Security Engineering	
Course Code: MIS-103 Contact Hours: L-3 T-0 P-2 Course Category: DCC	Credits: 4 Semester: 1

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 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 of this course, 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:

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

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

Fundamentals of Information Security	
Course Code: MIS-105 Contact Hours: L-3 T-0 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

Prerequisite: None

Course Outcomes: Upon successful completion, the students would be able:

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, Defences, 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	

Data Structures and Algorithm Analysis	
Course Code: MCS-107 Contact Hours: L-3 T-0 P-2 Course Category: DCC	Credits: 4 Semester: 1

Introduction:

This course is about teaching of various data structure designs & its implementations, analyzing the various algorithm strategies and designing of new algorithms for various classes of problems. It is intended to be a gentle introduction to how we specify data structure, algorithms, some of the design strategies, and many of the fundamental ideas used in algorithm analysis throughout the syllabus.

Course Objective:

- To build an understanding on the basics of core and advance data structure.
- To introduce the various strategies used in the algorithm design and their analysis.
- To teach the selection of data structure for a particular problem
- To teach students, how to write complex program using dynamic data structures

Pre-requisite: Students should have some programming experience. In particular, they should understand recursive procedures and simple data structures such as arrays and linked lists. Students should have some facility with proofs by mathematical induction.

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

CO1: Successfully design and implements the core and advance data structures
CO2: Successfully analyses the complexity associated with the various data structures
CO3: Analyse, design and implements the various proposed algorithm based on strategies.
CO4: Choose data structures for various complex 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
Algorithms performance analysis: Time and space complexity, Asymptotic Notations, Complexity Analysis Examples. **Linear Data Structures:** Arrays, Stacks, Queues, linked lists, **Recursion:** Solving recurrences.	
UNIT-II	**10 Hours**
Non-linear Data Structure: Trees, Traversals, Binary Search Trees, AVL tree, B-trees, B+ Tree, Red Black Tree. **Graph Algorithms:** DFS, BFS, Minimum Spanning Tree Algorithms, Shortestpath Algorithms.	
UNIT-III	**12 Hours**
Sorting and Searching Algorithms: Quick Sort, Merge Sort, Heap sort; Linear Search and Binary Search. **Hashing:** Hashing Functions, Collision Resolution Techniques	
UNIT-IV	**10 Hours**
Algorithm Strategies: Greedy paradigm with examples. Divide and conquer paradigm with examples. Dynamic-programming paradigm with examples. **NP Completeness:** P, NP, NP-complete, NP-Hard categories of problems, Cook's theorem.	

Text Books	
1	Y. Langsam et. al., "Data Structures using C and C++", Second Edition, PHI, 2015.
2	E. Horowitz, S. Sahani, Anderson-Freed "Fundamentals of Data Structures in C", Second Edition, University Press, 2008
3	T. H. Cormen, C. E. Leiserson, R. L. Rivest, Clifford Stein, "Introductionto Algorithms", 3rd Ed., PHI, 2011.
Reference Books	
1	R. L. Kruse, B. P. Leung, C. L. Tondo, "Data Structures and program design in C", PHI, 2010.
2	Ellis Horowitz and Sartaz Sahani, "Fundamental of Computer Algorithms", Galgotia Publications, 2009.
3	A. V. Aho, J. E. Hopcroft, J. D. Ullman, "The Design and Analysis ofComputer Algorithms", Addition Wesley, 2009.
4	D. E. Knuth, "The Art of Computer Programming", 2nd Ed., Addison Wesley, 2011.

Generic Open Elective	
Course Code: GEC-101 Contact Hours: 2-0-0 1-1-0 0-0-4 0-2-0 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. Generic Electives (GE) are introduced as part of the CBCS. The students can choose their preference from a pool of papers from various disciplines/subjects from NPTEL, departments of IGDTUW, or IGDTUW Incubation Centre-Anveshan Foundation. The courses should be recommended by the respective HoD and approved by the BoS. 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.

The maximum credit award will be 2 per year to the student's total credit score for a GEC. All the expenses including registration and certification fee shall be borne by the student. The duration of the GEC course shall be minimum 6 weeks, with a mode of evaluation and assessment. Students can enroll for one/two NPTEL courses, but credit is to be considered for one course only. The student should inform and take the consent of the HoD for pursuing the GEC, within 01 week of the start of the semester.

Apart from the categories, a student may pursue a research-based course under the supervision of a faculty. A duly constituted committee at the Department level will conduct the evaluation and submit the marks. New subjects/courses under GEC can be added from time-to-time after seeking necessary approval of the statutory bodies of the University.

Course Objectives:

- Students will have exposure to a new discipline/subject.
- Prepare students to look for inter-disciplinary research.
- GE can fulfil 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: Investigate future careers

CO2: Allow diligent students to improve their knowledge and area of weakness

CO3: Help students build a strong resume that shows students willingness and curiosities to the officials and employers

CO4: Electives take students into the real world that does not require academic papers or research. They not only learn to work independently, but they attain self-motivation, discipline, and confidence to achieve their goals.

Research Methodology	
Course Code: ROC-101 Contact Hours: L-3 T-0 P-0 Course Category: ROC	Credits: 3 Semester: 1

Introduction:

The course introduced the students to the research world. They will understand how to read and interpret a research paper. Also, this course will make then understand how to write their own research proposals.

Course Objectives:

- The purpose is to align the M. Tech. students with the research process of the rest of the world so that when they go for higher studies either in university or industry, they should be aware of how to communicate their research to the rest of the world and how to read and interpret the research work of others.
- The students will also become aware of metrics of how to evaluate the quality of different research works.
- The practical statistical tools will enhance their skills to apply mathematical tools to their research to interpret results and communicate in a common jargon.

Prerequisite: Knowledge of basic logic; Java/object-oriented programming, data structures and algorithms, Web technologies, such as URL, http, HTML, and XML-based technologies, Database technology such as, relational databases and SQL query language

Course Outcomes: Having successfully completed this course

CO1: The students will be able to write their own research proposal.

CO2: They will also have familiarity with research journals, how do the whole process work right from draft of a research paper to reviewer comments and publishing.

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
Objectives and Motivation of Research, Types of Research, Research Approaches, Significance of Research, Research Methods verses Methodology, Research and Scientific Method, Important of Research Methodology, Research Process, Criteria of Good Research, Problems Encountered by Researchers in India, Benefits to the society in general. Defining the Research Problem: Definition of Research Problem, Problem Formulation, Necessity of Defining the Problem, Technique involved in Defining a Problem.	
UNIT-II	**10 hours**
Literature Survey: Importance of Literature Survey, Sources of Information, Assessment of Quality of Journals and Articles, Information through Internet, Significance of ISSN, DOI, Impact Factor, Citations. Rules of Citation. Research Design: Meaning of Research Design, Need of Research Design, Feature of a Good Design, Important Concepts Related to Research Design, Different Research Designs, Basic Principles of Experimental Design, Developing a Research Plan, Design of Experimental Set-up, Use of Standards.	
UNIT-III	**11 hours**
Descriptive Statistics, Points of Central tendency, Measures of Variability, Measures of relationship, Inferential Statistics-Estimation, Hypothesis Testing. How to read data from multiple files, Interpretation of Data: Univariate Analysis, Tests for significance: Chi square, t-test, Regression modeling, Direct and Interaction effects, ANOVA, F-test, Time Series analysis, Autocorrelation and Autoregressive modeling. Inferential statistics: Normal Curve, Confidence Interval, Type1 and Type 2 errors.	
UNIT-IV	**11 hours**
Research Report Writing: Format of the Research report, Style of writing report, References/Bibliography/Webliography, Technical paper writing/Journal report writing. Survey Methods: Questionnaire method; Types of Questionnaires; Process of Questionnaire Designing; Advantages and Disadvantages of Questionnaire Method.	
Text Books	
1. C.R Kothari, "Research Methodology, Methods & Technique"; New Age International Publishers, 2004	
2. R. Ganesan, "Research Methodology for Engineers", MJP Publishers, 2011	
3. Y.P. Agarwal, "Statistical Methods: Concepts, Application and Computation", Sterling Publs., Pvt., Ltd., New Delhi, 2004	
4. Vijay Upagade and Aravind Shende, "Research Methodology", S. Chand & Company Ltd., New Delhi, 2009	

Advances in Machine Learning	
Course Code: MIS-102 Contact Hours: L-3 T-0 P-2 Course Category: DCC	Credits: 4 Semester: 2

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 introduce 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:

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, 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	**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 Neighbour 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.	

Applied Cryptography	
Course Code: MIS-104 Contact Hours: L-3 T-1 P-0 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.

Prerequisite: None

Course Outcomes:

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:

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

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

Text Books

1. W Stallings, “Cryptography and Network Security: Principles and Practice, 6/e”, Prentice Hall
2. B. Forouzan, D. Mukhopadhyay, "Cryptography and Network Security 2/e", Tata-McGraw Hill
3. Christof Paar, Jan Pelzl, “Understanding Cryptography: A textbook for students and practitioners, 1/e”, Springer
4. Bernard Menezes, “Network Security and Cryptography 2/e”, Cenege Learning

Reference Books

1. A. Menezes, P. van Oorschot, S. Vanstone. “Handbook of Applied Cryptography”, CRC press, 1997.
2. Douglas R. Stinson, “Cryptography: Theory and Practice 3/e”, CRC Press, 2006
3. B. Schneier. “Applied Cryptography”. Second Edition. John Wiley & Sons, Inc., 1996

Cyber Security and Forensics	
Course Code: MIS-106 Contact Hours: L-3 T-0 P-2 Course Category: DEC	Credits: 4 Semester: 2

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 Objective:

- 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 completion of the course the 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.	
Textbooks	
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	

Ethical Hacking	
Course Code: MIS-201 Contact Hours: L-3 T-0 P-2 Course Category: DCC	Credits: 4 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 Objectives:

- 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.

Prerequisite: Fundamentals of Information Security (MIS-105)

Course Outcomes: 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

CO3: Analyze and test ethical hacking tools and techniques

CO4: 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 quizes. 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 Defence”, 3rd Ed., Cengage Learning, 2016	
2. Rafay Baloch, “A Beginners Guide to Ethical Hacking”, 1st Ed., CRC Press, 2014	

Generic Open Elective	
Course Code: GEC-201 Contact Hours: 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. Generic Electives (GE) are introduced as part of the CBCS. The students can choose their preference from a pool of papers from various disciplines/subjects from NPTEL, departments of IGDTUW, or IGDTUW Incubation Centre-Anveshan Foundation. The courses should be recommended by the respective HoD and approved by the BoS. 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.

The maximum credit award will be 2 per year to the student's total credit score for a GEC. All the expenses including registration and certification fee shall be borne by the student. The duration of the GEC course shall be minimum 6 weeks, with a mode of evaluation and assessment. Students can enroll for one/two NPTEL courses, but credit is to be considered for one course only. The student should inform and take the consent of the HoD for pursuing the GEC, within 01 week of the start of the semester.

Apart from the categories, a student may pursue a research-based course under the supervision of a faculty. A duly constituted committee at the Department level will conduct the evaluation and submit the marks. New subjects/courses under GEC can be added from time-to-time after seeking necessary approval of the statutory bodies of the University.

Course Objectives:

- Students will have exposure to a new discipline/subject.
- Prepare students to look for inter-disciplinary research.
- GE can fulfil 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: Investigate future careers

CO2: Allow diligent students to improve their knowledge and area of weakness

CO3: Help students build a strong resume that shows students willingness and curiosities to the officials and employers

CO4: Electives take students into the real world that doesn't require academic papers or research. They not only learn to work independently, but they attain self-motivation, discipline, and confidence to achieve their goals.

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

Course Objectives:

- 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

Course Outcomes:

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

CO2: Implement and Analyse 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: MIS-253 Contact Hours: - Course Category: DCC	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.

Pedagogy:

The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/presentations and quizes. 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.

Dissertation – II / Project Work	
Course Code: MIS-252 Contact Hours: - Course Category: DCC	Credits: 8 Semester: 4

Course Objectives:

- 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

Course Outcomes:

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

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

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

Advanced Database Management Systems	
Course Code: MIS-108 Contact Hours: L-3 T-0 P-2 Course Category: DEC	Credits: 4 Semester: 2

Introduction:

Students study the basic and fundamentals of Database Management Systems at UG level, where they covers basics of RDBMS, Normalization, SQL, Transaction Management and Concurrency control techniques. However, since the complexity and size of databases is continuously increasing, advanced approaches to store and manage the data is required.

Course Objectives:

- To learn advanced and complex queries in SQL
- To learn PL/SQL with an emphasis on Exceptions handling, Cursors, Triggers, Procedures, Functions and Packages in PL/SQL
- To learn new approaches and trends in Databases like OODBMS, DDBMS, Multimedia database Management Systems and Big Data approaches.

Prerequisite: Understanding of Database Concepts and SQL

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

CO1: Write appropriate programs (Procedures/Functions/Triggers) at Server side for better, efficient and secure application development.

CO2: Implement various advanced concepts of Database management Systems like Object Oriented System, Distributed Database Systems and Multimedia Database Management Systems for database design.

CO3: Understand and use the unstructured big data along with concepts like Hadoop, Map Reduce, NoSQL, Pig and Hive for management and analytics.

Pedagogy:

The subject will be taught through lectures, presentations and working on case studies. Lab sessions will cover exercises on advanced SQL queries, PL/SQL programs, use of object oriented concepts in database designing along with hands on experiments on Big Data.

UNIT-I	**10 hours**
Fundamentals of Relational Model, Advanced SQL queries: Nested Queries, Joins, Correlated Queries, Views, Indexes, Sequence. PL/SQL: Exceptions, Cursors, Triggers, Functions, Procedures, Packages.	
UNIT-II	**11 hours**
Indexing &Hashing, B+ Tree Index Files, B-Tree Index Files, Dynamic & Static Hashing, Query Processing, Measures of Query cost, Selection Operation, Sorting, Join operation, evaluation of expressions, Query Optimization, Estimating Statistics of Expression Results, Transformation of Relational Expressions, Materialized Views	
UNIT-III	**11 hours**
Object Oriented and Object Relational Database Systems, Abstract Data Types, Varrying Array, Nested Tables. Distributed Databases, Homogeneous & Heterogeneous Databases, Distributed Data Storage, Distributed Transactions and their commit protocols, Concurrency Control in Distributed Data Bases, Decision Support Systems. Multimedia Databases, Mobile Data bases, Spatial Database.	
UNIT-IV	**10 hours**
Big Data-Volume, Velocity, Variety, Veracity, Types and Sources of Big Data OLAP & RTAP, Data Exploration, Data Summaries, Data Visualization, Tools for Big Data Analytics, No SQL, Hadoop, Map Reduce, Gephi	
Text Books	
1. Fundamentals of Database System, by Elmasri Ramez and Navathe Shamkant, Pearson, 7th Edition, 2017	
2. Big Data Analytics, Radha Shankarmani and M. Vijayalakshmi, Wiley, 2nd Edition 2016	
Reference Books	
1. Database System Concepts, by Abraham Silberschatz and Hank Korth, McGraw Hill Publication, 6th Edition, 2013	
2. Introducing Data Science: Big Data, Machine Learning, and More, Using Python Tools, by Davy Cielen and Arno D.B. Meysman, Dreamtech Publication, 2016	

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

Introduction:

Biometrics systems are preferred over traditional identification and verification methods to reduce the fraud and make system more secure among intelligence, security, e-commerce etc. This course introduces students to the basic principles and methods used for Computer Vision. The objective is to provide students with the scientific foundations needed to design, implement, and evaluate large scale computer vision systems.

Course Objectives:

- Understand the scope and options of Machine Learning in computer vision: Face detection using Adaboost, Object detection using parts.
- Students will learn how the technologies should be used to use in the human recognition

Prerequisite: Basic mathematics - knowledge and ability to use calculus, probability, and statistics are essential. The student should have experience in a high-level programming language such as Matlab or C/C++.

Course Outcomes: After completing the course students will be able to:

CO1: Understand basic image processing.

CO2: Analyse different problems in image processing.

CO3: Understand advanced concepts in image processing.

Pedagogy:

Lectures will be supported with case studies and real time applications wherever applicable. Also, emphasis will be given on developing applications (system software) by writing programs.

UNIT-I	10 hours
Introduction to Computer Vision, Image Formation: Geometric primitives and transformations, Photometric image formation, The digital camera Image processing: Point operators, Linear filtering, More neighbourhood operators, Fourier transforms, Pyramids and wavelets, Geometric transformations, Global optimization Feature detection and matching, Points and patches, Edges, Lines	
UNIT-II	**12 hours**
Image Segmentation: Active contours, Split and merge , Mean shift and mode finding , Normalized cuts, Graph cuts and energy-based methods Feature-based alignment: 2D and 3D feature-based alignment, Pose estimation, Geometric intrinsic calibration Structure from motion: Triangulation, Two-frame structure from motion , Factorization, Bundle adjustment, Constrained structure and motion Dense motion estimation: Translational alignment, Parametric motion, Spline-based motion, Optical flow, Layered motion Image stitching: Motion models, Global alignment, Compositing	
UNIT-III	**10 hours**
Computational photography: Photometric calibration, High dynamic range imaging, Super- resolution and blur removal, Image matting and compositing, Texture analysis and synthesis. Stereo correspondence: Epipolar geometry, Sparse correspondence, Dense correspondence, Local methods, Global optimization, Multi-view stereo. 3D reconstruction: Shape from X, Active range finding, Surface representations, Point-based representations, Volumetric representations, Model-based reconstruction, Recovering texture maps and albedos	
UNIT-IV	**10 hours**
Image-based rendering: View interpolation, Layered depth images, Light fields and Lumigraphs, Environment mattes, Video-based rendering Recognition: Object detection, Face recognition, Instance recognition, Category recognition, Context and scene understanding, Recognition databases and test sets Future applications of computer vision	
Text Books	
1. Richard Szeliski, Computer Vision: Algorithms and Applications, Springer-Verlag London Limited 2011.	
2. Computer Vision: A Modern Approach, D. A. Forsyth, J. Ponce, Pearson Education, 2015.	
Reference Books	
1. Digital Image Processing and Analysis: Application with MATLAB and CVIPtools, 3rd Edition, SE Umbaugh, Taylor&Francis/CRC Press, 2018	

Blockchain Fundamentals	
Course Code: MIS-114 Contact Hours: L-3 T-0 P-2 Course Category: DEC	Credits: 4 Semester: 2

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

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

Course Outcomes: The students will be able to

CO1: Understand Blockchain and Distributed Ledger Technology.

CO2: Explain the elements of trust in Blockchain using validation, verification, and consensus.

CO3: Develop blockchain based solutions and write smart contracts.

CO4: Create application areas, current practices and research activity using Blockchain technology.

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	**12 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	**10 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	**10 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	**10 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	

Semantic Web	
Course Code: MIS-118 Contact Hours: L-3 T-1 P-0 Course Category: DEC	Credits: 4 Semester: 2

Introduction: The knowledge contained in the World Wide Web is available in interlinked documents written in natural language. To make use of this knowledge, technologies such as natural language processing, information retrieval, data and knowledge mining must be applied. Semantic Web technologies follow an alternative approach by complementing web documents with explicit semantics based on formal knowledge representations, such as ontologies. This course provides an introduction and practical tutorial on the RDF-based semantic annotation of Web resources and services for the Semantic Web, Linked Data and Ontology Engineering; and also reviews some modern applications of these methods and techniques for Web-based intelligent applications and services.

Course Objectives:

- To offer an introduction to knowledge and logic-based information technologies, using logic programming as the primary example of knowledge-based reasoning, and the Semantic Web as the primary example of a knowledge-based application area.
- To introduce the W3C standard Web Ontology Language, OWL, and its underlying Description Logics
- To provide experience using a set of established patterns for developing OWL ontologies
- To understand linked data technologies and applications

Prerequisite: Knowledge of basic logic; Java/object-oriented programming, data structures and algorithms, Web technologies, such as URL, http, HTML, and XML-based technologies, Database technology such as, relational databases and SQL query language

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

CO1: Apply RDF, OWL, and SWRL syntax for semantic annotations and rule specification for web resources.

CO2: Describe linked data principles and architecture, as in dbpedia, Wiki, FOAF etc.
CO3: Analyse linked data and visualization using SPARQL with R/Python.

CO4: Develop a deep insight to the various state-of-the-art technologies of semantic search engine, semantic web browser and semantic recommender systems.

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 will be adopted.

UNIT-I	**10 hours**
Knowledge Engineering and the Web of Data, Semantic Web standards: Uniform Resource Identifier (URI) RDF (Resource Description Framework); Ontology Engineering; OWL (Web Ontology Language), SPARQL, Semantic Web mission; concepts of semantic interoperability, integration and automation; concept of metadata and ontology; description logics	
UNIT-II	**11 hours**
Methods for developing and evaluating ontologies. Application development using the OWL API, Tableaux Algorithm, DL Reasoning Problems, Canonical forms, Resolution (PL/FOL), OWL and RDF(S) Semantics Basics, Open and Closed world assumptions, Rules for inferring knowledge, First order Logic, RDF-S semantics, Web Ontology Language(OWL), Semantic Web Rule Language(SWRL), Friend-of-a-Friend(FOAF)	
UNIT-III	**11 hours**
Query languages SPARQL, SWRL (Semantic Web Rules Language); Semantic Technology; Rules, Protége, Ontology Alignment, Ontology Evaluation, More Ontology Design Methodologies, Metadata, Fundamentals of Ontology and its types, monolithic vs. modular ontology, ontology design methodology, ontology learning, ontology learning from text, automated ontology learning process	
UNIT-IV	**10 hours**
Linked Data Engineering, Semantic (Web) infrastructure, applications and Services; Relation to Big Data and Industry 4.0, Linked Data Programming, Semantic Annotation, Named Entity Resolution, Semantic Search, Exploratory Search, Linked Data Analytics, Semantic Recommendations	
Text Books	
1. Grigoris Antoniou, Paul Groth, Frank van Harmelen and Rinke Hoekstra, A Semantic Web Primer, MIT Press, 3rd Edition (September, 2012).	
2. David Wood, Marsha Zaidman, Luke Ruth, and Michael Hausenblas, Linked Data: Structured Data on the Web, Manning Publications; 1st Edition (January 24, 2014).	
3. Bob DuCharme, Learning SPARQL: Querying and Updating with SPARQL 1.1, O'Reilly Media; 2nd Edition (July 18, 2013)	
Reference Books	
1. Liyang Yu, A Developer's Guide to the Semantic Web, Springer Science & Business Media, 2011	
2. SteffanStaab and Rudi Studer , Handbook on Ontologies", Springer Science & Business Media, 2010	

Security Testing and Risk Management	
Course Code: MIS-120 Contact Hours: L-3 T-0 P-2 Course Category: DEC	Credits: 4 Semester: 2

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 of this course, 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: Develop a deep insight to the various state-of-the-art technologies of semantic search engine, semantic web browser and semantic recommender systems.

CO5: Assess, evaluate and analyse risk of a software applications using standard Rsik assessment and Management Framework.

Pedagogy:

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

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.	
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	

Security Patterns	
Course Code: MIS-205 Contact Hours: L-3 T-0 P-2 Course Category: DEC	Credits: 4 Semester: 3

Introduction:

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

Course Objectives:

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

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

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

CO1: Learn fundamental concepts of security patterns.

CO2: Identify and apply the appropriate security pattern to solve real-time problems.

CO3: Know how to format a document using Document editor.

CO4: Label out the solutions to design problems using creational, structural and behavioural patterns.

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 will be adopted.

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

Advanced Network Technology	
Course Code: MIS-209 Contact Hours: L-3 T-0 P-2 Course Category: DEC	Credits: 4 Semester: 3

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, the students should 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 the existing real life cyber security issues and how they are solved. Use of ICT and web-based sources 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 Adhoc Network, Data Center Networking, Delay Tolerant Networking, Home Networking, Green Networking, Internet of Things, Software Defined Networking, Web-Scale Networking: Distributed Cloud Computing and Virtual Machine Migration.	
UNIT-IV	**10 hours**
Content Networks: Video Streaming, Wireless Networking: Wireless Mesh, Geographic Routing, Network Security principles, Security related issues in wireless networks, Public and Private Key Cryptography, Key distribution protocols. Digital Signatures, and digital certificates, Firewall, Next Generation Fire wall, Radio Networks, Opportunistic Network	
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, 201	

Cyber Law and Rights	
Course Code: MIS-211 Contact Hours: L-3 T-1 P-0 Course Category: DEC	Credits: 4 Semester: 3

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

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

Security and Privacy in Social Networks	
Course Code: MIS-213 Contact Hours: L-3 T-1 P-0 Course Category: DEC	Credits: 4 Semester: 3

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	

Software Defined Networks	
Course Code: MIS-215 Contact Hours: L-3 T-1 P-0 Course Category: DEC	Credits: 4 Semester: 3

Introduction:

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

Course Objectives:

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

Prerequisite: Basic understanding of data communication and computer networks

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

CO1: Examine the challenges and opportunities associated with adopting SDN compared to traditional approaches to networking.

CO2: Analyse the functions and components of the SDN architecture.

CO3: Discuss the major requirements of the design of an SDN protocol.

CO4: Design and create an SDN network consisting of SDN switches and a centralised controller.

Pedagogy:

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

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

Cloud Computing Architecture and Security	
Course Code: MIS-217 Contact Hours: L-3 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: On successful completion of this course, the students should be able to:

CO1: To articulate key concepts of cloud computing and computing techniques, strength and limitations of cloud computing with possible application domains.

CO2: To identify the architecture and infrastructure of cloud computing including SaaS, PaaS, IaaS, public cloud, private cloud and hybrid cloud.

CO3: To interpret various data, scalability and cloud services to acquire efficient database for cloud storage.

CO4: To explain the core issues of cloud computing such as security, privacy and interoperability and deal with controlling mechanism for accessing sage cloud service.

Pedagogy:

Subject lectures would be delivered via class discussions, tutorials, slide-shows, white board and online quizzes. Students would be encouraged to take an individual case study from Industry 4.0. Students would be guided to survey the state-of-the-art and undertake a research project.

UNIT-I	**10 hours**
Introduction: Introduction of Cloud Computing (CC), NIST definition of CC, Peer-to-Peer Approach, Parallel-Distributed Computing, Cluster and Grid Computing, Evolution of CC from 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, Green CC, Elastic Computing, Enterprise CC, CloudStack. 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	**10 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	**10 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	**10 hours**
Advanced Security Issues: Security Concerns-Threats to Infrastructure, Data and Access Control, Cloud Information Security Objectives: Confidentiality, Accessibility, Organizational Security and Privacy Requirements, Client-Side Computing Environment Requirements, Integrity, Cloud Security Design Principles, Secure Cloud Software Testing, Vulnerability Assessment Tools, 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, VM Security Techniques, Information Privacy, Laws and Legal Matters in Cloud Computing, Mobile Cloud Computing, Cloud Computing Environment Open-Stack, 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	