

Teaching Scheme of B.Tech.–IV (CSE) (Semester VIII)

Sr. No.	Course	Code	Credit	Teaching Scheme			Examination Scheme			Total
				L	T	P	L	T	P	
1	Core Elective-5	CS4XX	3	3	0	0	100	0	0	100
2	Core Elective-6	CS4YY	3	3	0	0	100	0	0	100
3	Core Elective-7	CS4ZZ	3	3	0	0	100	0	0	100
4	Cyber Law and Forensics (Core-16)	CS402	4	3	0	2	100	0	50	150
5	Project	CS404	6	0	0	12	0	0	300	300
	Total		19	12	0	14	400	0	350	750
	Total Contact Hours per week			26						

Practical Examination Scheme (Internal 50% and External 50%)

Core Elective-5 (CS4XX):

1	Social Network Analysis (CS422)	4	Cellular Network and Mobile Computing (CS428)
2	Network and System Security (CS424)	5	System Analysis and Simulation (CS432)
3	Advanced Computer Architecture (CS426)		

Core Elective-6 (CS4YY):

1	Big Data Analytics (CS434)	4	Advanced Database Management System (CS442)
2	Deep Learning (CS436)	5	Web Engineering (CS444)
3	Advanced Compiler Design (CS438)		

Core Elective-7 (CS4ZZ):

1	Foundations of Automatic Verification (CS446)	4	Research Methodologies (CS454)
2	Secure Software Engineering (CS448)	5	Ethical Hacking (CS456)
3	Animation & Rendering (CS452)		

B.Tech. IV (CSE) Semester – VIII
SOCIAL NETWORK ANALYSIS (CORE ELECTIVE - 5)
CS422

Scheme

L	T	P	Credit
3	0	0	03

1. <u>Course Outcomes (COs):</u>	
At the end of the course, students will be able to	
CO1	acquire knowledge about the social network data, relations among data, identification of network structure and relevant programming.
CO2	apply the model for the solution of social network problem statement to generate data sets, relations, graph.
CO3	analyze the problem solution for social network analysis considering social influence.
CO4	evaluate programming solutions with different aspects of social network analysis.
CO5	design an innovative optimised solution for the social network application problem using network dynamics.

2. Syllabus

- INTRODUCTION (08 Hours)**
Introduction of Social Networks, Social Networks Data, Development of Social Network Analysis, Analyzing Social Network Data, Formal Methods, Paths and Connectivity, Graphs to Represent Social Relations, Working with Network Data, Network Datasets, Strong and Weak Ties, Closure, Structural Holes, and Social Capital, Measures for Social Network Analysis.
- SOCIAL INFLUENCE (09 Hours)**
Homophily, Mechanisms Underlying Homophily, Social Influence, Affiliation, Identification of Roles, Tracking Link Formation in OnLine Data, Spatial Model of Segregation - Positive and Negative Relationships , Structural Balance, Applications of Structural Balance, Weaker Form of Structural Balance.
- WEB INFORMATION NETWORKS (09 Hours)**
The Structure of the Web, World Wide Web, Information Networks, Hypertext, and Associative Memory, Web as a Directed Graph, Bow-Tie Structure of the Web, Link Analysis and Web Search, Searching the Web: Ranking, Link Analysis using Hubs and Authorities, Page Rank, Link Analysis in Modern Web Search, Applications, Spectral Analysis, Random Walks, and Web Search, Social Network Visualization.
- SOCIAL NETWORK MINING (08 Hours)**
Social Networks, Geography, Neighbourhood Effects, Clustering of Social Network Graphs: Betweenness, Girvan Newman Algorithm, Discovery of Communities, Cliques and Bipartite Graphs, Graph Partitioning Methods, Matrices, Eigen Values, Simrank.

● **NETWORK DYNAMICS** (08 Hours)

Network Effects of Local Social Networks and Global Social Networks, Spread of Behaviour, Cascading Behaviour in Networks: Diffusion in Networks, Modelling Diffusion, Cascades and Cluster, Thresholds, Extensions of the Basic Cascade Model, Six Degrees of Separation, Structure and Randomness, Decentralized Search, Empirical Analysis and Generalized Models, Analysis of Decentralized Search, Problem Solving.

(Total Contact Time = 42 Hours)

3. Books Recommended:

1. Jure Leskovec, Anand Rajaraman, Jeffrey D. Ullman, "Mining of Massive Datasets", Cambridge University Press, 2/E, 2014, ISBN: 9781316638491.
2. Borgatti, S. P., Everett, M. G. & Johnson, J. C., "Analyzing social networks", SAGE Publications Ltd; 1/E, 2013, ISBN: 9781446247419.
3. David Easley and Jon Kleinberg, "Networks, Crowds, and Markets: Reasoning about a highly connected world", Cambridge Univ. Press, 2010, ISBN: 9780521195331.
4. Robert A., Hanneman and Mark Riddle, "Introduction to social network methods", University of California, 2005.
5. John Scott, "Social Network Analysis: A Handbook", SAGE Publications Ltd; 2/E, 2000, ISBN: 9780761963394.

ADDITIONAL REFERENCE BOOKS

1. Wasserman S. & Faust K., "Social Network Analysis: Methods and Applications", Cambridge University Press, 1/E, 1994, ISBN: 9780521387071.

B.Tech. IV (CSE) Semester – VIII
NETWORK AND SYSTEM SECURITY (CORE ELECTIVE - 5)
CS424

Scheme

L	T	P	Credit
3	0	0	03

1. <u>Course Outcomes (COs):</u> At the end of the course, students will be able to	
CO1	gain knowledge of network and system security attacks and its prevention mechanisms.
CO2	apply different security mechanisms for given application scenario.
CO3	perform security analysis of network and system security protocols.
CO4	evaluate security protocols for different metrics like functionality, cost and efficiency.
CO5	design and integrate security protocols depending on organization's requirement.

2. Syllabus

- **INTRODUCTION (04 Hours)**
Introduction to Network and System Security, Security Attacks, Security Requirements, Confidentiality, Integrity, and Availability, Security Mechanisms, NIST Security Standards, Assets and Threat Models.
- **REVIEW OF CRYPTOGRAPHIC TOOLS (04 Hours)**
Number Theory, Prime Numbers, Modular Arithmetic, Confidentiality with Symmetric Encryption, Message Authentication and Hash Functions, Public-Key Encryption, Digital Signatures and Key Management, Random and Pseudorandom Numbers.
- **SYSTEM SECURITY (10 Hours)**
User Authentication - Means of Authentication, Password-Based Authentication, Token-Based Authentication, Biometric Authentication, Remote User Authentication, Access Control-Access Control Principles, Subjects, Objects, and Access Rights, Discretionary Access Control, Example: UNIX File Access Control, Role-Based Access Control, Database Security-The Need for Database Security, Database Access Control, Inference, Statistical Databases, Database Encryption, Cloud Security, Malicious Software, Intruders, Denial of Service and Distributed Denial of Service attacks, Intrusion Detection and Prevention.
- **SOFTWARE SECURITY AND TRUSTED SYSTEMS (12 Hours)**
Buffer Overflow-Stack Overflows, Defending Against Buffer Overflows, Other Forms of Overflow Attacks, Software Security-Software Security Issues, Handling Program Input, Writing Safe Program Code, Interacting with the Operating System and Other Programs, Handling Program Output, Operating System Security-System Security Planning, Operating Systems Hardening, Application Security, Security Maintenance, Linux/Unix Security, Windows Security, Virtualization Security, Trusted Computing and Multilevel Security-The Bell-LaPadula Model for Computer Security, Other Formal Models for Computer Security,

The Concept of Trusted Systems, Application of Multilevel Security, Trusted Computing and the Trusted Platform Module, Common Criteria for Information Technology Security Evaluation, Assurance and Evaluation.

- **NETWORK SECURITY** **(10 Hours)**

Internet Security Protocols and Standards-Secure E-mail and S/MIME, Pretty Good Privacy (PGP), Domain Keys Identified Mail, Secure Sockets Layer (SSL) and Transport Layer Security (TLS), HTTPS, IPv4 and IPv6 Security, IPSec Protocol, Internet Authentication Applications-Kerberos, X.509, Public-Key Infrastructure, Federated Identity Management, Wireless Network Security-Wireless Security Overview, IEEE 802.11 Wireless LAN Overview, IEEE 802.11i Wireless LAN Security, Network Management Security-SNMP Protocol.

- **ADVANCED TOPICS** **(02 Hours)**

(Total Contact Time = 42 Hours)

3. Books Recommended:

1. William Stallings, Computer Security: Principles and Practice, 2/E, Pearson, 2012.
2. John Vacca, Network and System Security, 2/E, Elsevier, 2013.
3. William Stallings, Network Security Essentials: Applications and Standards, Prentice Hall, 4th edition, 2010.
4. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 2001.
5. William Stallings, Cryptography and Network Security, 7/E, Pearson, 2018.

B.Tech. IV (CSE) Semester – VIII
DEEP LEARNING (CORE ELECTIVE - 6)
CS436

Scheme

L	T	P	Credit
3	0	0	03

1. <u>Course Outcomes (COs):</u> At the end of the course, students will be able to	
CO1	understand fundamental principles, theory and approaches for learning with deep neural networks.
CO2	learn different types of Neural Network and Deep Neural Networks.
CO3	apply NN and DNN for various learning tasks in different domains.
CO4	evaluate various NN and DNN by performing complex statistical analysis for DL techniques.
CO5	design DL algorithms for real-world problems.

2. Syllabus

- **INTRODUCTION TO DEEP LEARNING (02 Hours)**
Basics of Human learning, Attributes of learning algorithms, Applications, Learning techniques, Types of Learning algorithms, Basics of Deep learning.
- **NEURAL NETWORKS BASICS (08 Hours)**
Biological Neuron, Idea of Computational Units, Output vs Hidden Layers; Linear vs Nonlinear Networks, McCulloch–Pitts Model, Thresholding Logic, Linear Perceptron, Perception Learning Algorithm, Linear Separability. Convergence Theorem for Perception Learning Algorithm, Learning via Gradient Descent, Logistic Regression, Back Propagation Models, Feed Forward Model Empirical Risk Minimization, Regularization, Auto Encoders, Continuous and Discrete Distributions; Maximum Likelihood, Cost Functions, Hypotheses and Tasks; Training Data; Cross Entropy, Bias-variance Trade Off, Regularization, Activation Function : Sigmoid, Tanh, RELU, Softmax; Types of Neural Network : Feed Forward Neural Network , Radial Basis Function Neural Network, Convolution Neural Network, Recurrent Neural Network(RNN) Long Short Term Memory, Modular Neural Network; Simple Word Vector Representations: Word2vec, GloVe.
- **DEEP NEURAL NETWORKS (12 Hours)**
Deep Learning Models : Restricted Boltzmann Machines, Deep Belief Nets, Convolutional Model; Deep Neural Networks: Difficulty of Training Deep Neural Networks, Greedy Layerwise Training; Better Training of Neural Networks: Newer Optimization Methods for Neural Networks (Adagrad, Adadelta, Rmsprop, Adam, NAG), Second Order Methods for Training, Saddle Point Problem in Neural Networks, Regularization Methods (Dropout, Drop Connect, Batch Normalization); Recurrent Neural Networks: Back Propagation Through Time, Long Short Term Memory, Gated Recurrent Units, Bidirectional LSTMs, Bidirectional RNNs ;Convolution Neural Networks: LeNet, AlexNet; Generative models: Restrictive Boltzmann Machines (RBMs), Introduction to MCMC and Gibbs Sampling, Gradient Computations in RBMs, Deep Boltzmann

Machines.

- **RECENT TRENDS** **(12 Hours)**

Auto Encoders (Standard, Denoising, Contractive, etc), Variational Auto Encoders, Adversarial Generative Networks, Maximum Entropy Distributions, Guest Lecture, Generative Adversarial Networks, Multi-task Deep Learning, Multi-view Deep Learning.

- **APPLICATIONS** **(08 Hours)**

Vision, NLP, Speech; Deep Learning Platforms and Software Libraries:-H2O.ai, DatoGraphLab, Theano, Caffe, TensorFlow etc.

(Total Contact Time: 42 Hours)

3. Books Recommended:

1. Ian Goodfellow and Yoshua Bengio and Aaron Courville, “Deep Learning (Adaptive Computation and Machine Learning series)”, MIT Press, 2016.
2. Russell, S. and Norvig, N. “Artificial Intelligence: A Modern Approach”, 3rd Edition, Prentice Hall Series in Artificial Intelligence Pearson, 2015.
3. Christopher M. Bishop, “Pattern Recognition and Machine Learning (Information Science and Statistics)”, 3rd Edition, Springer, 2016.
4. Raúl Rojas, “Neural Networks - A Systematic Introduction”, 2nd Edition, Springer-Verlag, Berlin, New-York, 2013.
5. Nikhil Buduma, Nicholas Locascio, “Fundamentals of Deep Learning: Designing Next-Generation Machine Intelligence Algorithms”, 1st Edition, O’reily, 2017.

B.Tech. IV (CSE) Semester – VIII
ADVANCED DATABASE MANAGEMENT SYSTEMS
(CORE ELECTIVE - 6)
CS442

Scheme

L	T	P	Credit
3	0	0	03

1. Course Outcomes (COs):

At the end of the course, students will

CO1	understand advanced database techniques for storing a variety of data with various database models.
CO2	apply various database techniques/functions with Object Oriented approach to design database for real life scenarios.
CO3	analyse the problem to design database with appropriate database model.
CO4	evaluate methods of storing, managing and interrogating complex data.
CO5	develop web application API's, distributed databases with the integration of various programming languages.

2. Syllabus

● **DISTRIBUTED DATABASE CONCEPTS** **(06 Hours)**

Overview of Client - Server Architecture and its Relationship to Distributed Databases, Concurrency Control Heterogeneity Issues, Persistent Programming Languages, Object Identity and its Implementation, Clustering, Indexing, Client Server Object Bases, Cache Coherence.

● **PARALLEL DATABASES** **(06 Hours)**

Parallel Architectures, Performance Measures, Shared Nothing/Shared Disk/Shared Memory Based Architectures, Data Partitioning, Intra-operator Parallelism, Pipelining, Scheduling, Load Balancing.

● **QUERY PROCESSING** **(06 Hours)**

Index Based, Cost Estimation, Query Optimization: Algorithms, Online Query Processing and Optimization, XML, DTD, XPath, XML Indexing, Adaptive Query Processing.

● **ADVANCED TRANSACTION MODELS** **(06 Hours)**

Save Points, Sagas, Nested Transactions, Multilevel Transactions, Recovery: Multilevel Recovery, Shared Disk Systems, Distributed Systems 2PC, 3PC, Replication and Hot Spares, Data Storage, Security and Privacy Multidimensional K- Anonymity, Data Stream Management.

● **MODELS OF SPATIAL DATA** **(05 Hours)**

Conceptual Data Models for Spatial Databases (e.g. Pictogram Enhanced ERDs), Logical Data Models for Spatial Databases: Raster Model (Map Algebra), Vector Model, Spatial Query

Languages, Need for Spatial Operators and Relations, SQL3 and ADT, Spatial Operators, OGIS Queries.

- **WEB ENABLED APPLICATIONS** **(05 Hours)**
Review of 3-Tier Architecture - Typical Middle-ware Products and Their Usage. Architectural Support for 3 -Tier Applications: Technologies Like RPC, CORBA, COM, Web Application Server - WAS Architecture Concept of Data Cartridges - JAVA/HTML Components, WAS.
- **OBJECT ORIENTED DATABASES** **(04 Hours)**
Notion of Abstract Data Type, Object Oriented Systems, Object Oriented DB Design. Expert Databases: Use of Rules of Deduction in Databases, Recursive Rules.
- **ADVANCED TOPICS** **(04 Hours)**
No SQL Databases, Unstructured Databases, Couchbase, MangoDB, Cassandra, Redis, Memcached.

(Total Contact Time: 42 Hours)

3. Books Recommended:

1. R. Elmasri and S. Navathe, "Fundamentals of Database Systems", 5th Edition, Benjamin-Cummings Pearson Education India, 2007.
2. Avi Silberschatz, Hank Korth, and S. Sudarshan, "Database System Concepts", 5th Edition, McGraw Hill, 2005.
3. S. Shekhar and S. Chawla, "Title Spatial Databases: A Tour", 1st Edition, Prentice Hall, 2003.
4. Hector Garcia-Molina, Jeff Ullman, and Jennifer Widom, "Database Systems", 2nd Edition, Pearson, 2008.
5. Carlos Coronel, Steven Morris, "Database Systems: Design, Implementation, & Management", 11th Edition, Cengage Learning, 2014.

B.Tech. IV (CSE) Semester – VIII
SECURE SOFTWARE ENGINEERING (CORE ELECTIVE - 7)
CS448

Scheme

L	T	P	Credit
3	0	0	03

1. Course Outcomes (COs):

At the end of the course, students will be able to

CO1	understand the security field and its key concept.
CO2	catch attack patterns.
CO3	analyse the risk behind any system/code.
CO4	evaluate the attack as well as cybercrimes.
CO5	design a system with minimal risk and attack possibilities.

2. Syllabus

● **INTRODUCTION (04 Hours)**

Software Security, Security in SDLC, Review of Software Engineering Concepts, SDLC, Software Qualities, Interdependence of Software Qualities, Security as a Software Quality, Review of Information Security Concepts, Software Security vs. Information Security vs. Application Security, Terminologies, The Trinity of Trouble viz. Connectivity, Extensibility and Complexity, Studies of Various Catastrophes Due to Insecure software, Model Based Security Engineering, Three Pillars of Software Security, Security in Software Lifecycle.

● **ATTACKS AND TYPES OF ATTACKERS (06 Hours)**

Attacks-Types, Methods, Attacks in Each Phase of Software Life Cycle, Motivation for Attackers, Methods for Attacks: Malicious Code, Hidden Software Mechanisms, Social Engineering Attacks, Physical Attacks, Non-malicious Dangers to Software, Attacks in Each Phase of Software Life Cycle, Security Vulnerabilities and Attack Taxonomy in Internet of Things and Cyber Physical Systems, Attack Trees, Attack Trees for BGP, PGP, PGP Probable Vulnerabilities.

● **SECURITY VULNERABILITIES-I (06 Hours)**

Introduction to Stack Analysis, Hands on Stack Analysis using gcc Compiler and gdb Debugger Tool, Methods of Attack, Taxonomy of Security Vulnerabilities, Introduction to Code Reviews and Static Informal Reviews, Formal Inspections. Code Coverage and Code Coverage Criteria viz. Statement Coverage, Branch Coverage, Condition Coverage, Path Coverage, Illustrations.

● **SECURITY VULNERABILITIES-II (04 Hours)**

Format String Vulnerabilities, Race Conditions Vulnerability, Examples of TOCTOU Race Conditions in Linux Environment, Code Injection and its Types, SQL Injection, Interpreter Injection; Weak Session Cookies, Buffer Over flows, Hidden Form Fields, Fail Open Authentication, Cross-site Scripting.

● **INTRODUCTION TO PETRINET (04 Hours)**

Petrinet as a Modelling Tool, Graphical Notations, Modelling Deadlocks and Starvation, Coloured

Petrinets, Simulations of Real time Applications using Petrinets

- **INTEGRATING SECURITY INTO SDLC. (02 Hours)**

Risk Management and Threat Modelling Methodologies, Software Risk Assessment and Threat Modelling Methodologies, Secure Development Cycle Activities and Practices.

- **USECASE MODELLING (04 Hours)**

Usecases, Sequence Diagram, Collaboration Diagram, Illustrations of Kerberos and SET Through Sequence Diagram.

- **ATTACK PATTERNS (04 Hours)**

The Attack Patterns, Illustrations, Review of Design Patterns in SE and Multi-tier architecture, Attack Proles, Attack Proles from Attack Patterns, Usage of Attack Proles, Using Attack Patterns in Attack Proles, Generating Attack Patterns, Case Studies, Abuse Cases, Misuse Cases, Using Attack Patterns to Generate an Abuse Case Model and Anti-Requirements, Finite State Machines for Security Requirements, Case Studies, Security Patterns.

- **ARCHITECTURAL RISK ANALYSIS (04 Hours)**

Introduction to UMLSEC AND SECUREUML, Risk Analysis using Z for Secure Specifications, Introduction To Penetration Testing.

- **SECURE PROGRAMMING (04 Hours)**

Common Software Security Bugs and Coding Errors.

(Total Contact Time: 42 Hours)

3. Books Recommended:

1. Gary McGraw, "Software Security: Building Security", 2nd Edition, Addison Wesley Software Security Series, 2006.
2. Theodor Richardson, Charles Thies, "Secure Software Design", 2nd Edition, Jones and Bartlet Learning, 2013.
3. Ghezzi, Jazayeri, Mandrioli, "Fundamentals of Software Engineering", 2nd Edition, Pearson EDU, 2003.
4. Mark Merkow, "Secure, Resilient, and Agile Software Development", 1st Edition, Auerbach Publications, 2019.
5. Jason Grembi, "Secure Software Development: A Security Programmer's Guide", 1st Edition, Cengage Learning, 2008.

B.Tech. IV (CSE) Semester – VIII
ETHICAL HACKING (CORE ELECTIVE - 7)
CS456

Scheme

L	T	P	Credit
3	0	0	03

1. <u>Course Outcomes (COs):</u> At the end of the course, students will be able to	
CO1	acquire knowledge of core concepts related to information security and ethical hacking.
CO2	install, configure, and use different state of the art hacking software on a closed network environment.
CO3	analyze the vulnerabilities related to computer system and networks using state of the art tools and technologies.
CO4	evaluate best practices in information security to maintain confidentiality, integrity and availability.
CO5	implement effective solutions for ethical hacking in different environments.

2. Syllabus

- **INTRODUCTION (09 Hours)**
Ethical Hacking: Introduction, Networking & Basics, Foot Printing, Google Hacking, Scanning, Windows Hacking, Linux Hacking, Trojans & Backdoors, Virus & Worms.
- **INFORMATION AND NETWORK SECURITY (09 Hours)**
Proxy & Packet Filtering, Denial of Service, Sniffer, Social Engineering System and Network Vulnerability and Threats to Security , Various Types of Attack and the Various Types of Attackers in the Context of the Vulnerabilities Associated With Computer and Information Systems and Networks Physical Security, Steganography.
- **ETHICAL HACKING – 1 (12 Hours)**
Cryptography, Wireless Hacking, Firewall & Honeypots, IDS & IPS, Vulnerability, Penetration Testing, Session Hijacking, Hacking Web Servers, SQL Injection, Cross Site Scripting, Exploit Writing, Buffer Overflow.
- **ETHICAL HACKING – 2 (12 Hours)**
Reverse Engineering, Email Hacking, Incident Handling & Response, Bluetooth Hacking, Mobile Phone Hacking Basic Ethical Hacking Tools and Usage of These Tools in a Professional Environment. Legal, Professional and Ethical Issues Likely to Face the Domain of Ethical Hacking. Ethical Responsibilities, Professional Integrity and Making Appropriate Use of the Tools and Techniques Associated With Ethical Hacking.

(Total Contact Time: 42 Hours)

3. Books Recommended:

1. Dominic Chell, Tyrone Erasmus, Shaun Colley, Ofllie Whitehouse," The Mobile Application Hacker's Handbook", 2nd Edition, Wiley, 2015.
2. Michael Gregg, "Certified Ethical Hacker (CEH) Cert Guide", 2nd Edition, Pearson India, 2014.
3. Rafay Baloch, "Ethical Hacking and Penetration Testing Guide", 2nd Edition, CRC Press, 2017.
4. Allen Harper, Shome Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, Terron Villiams "Gray Hat Hacking The Ethical Hakers Handbook", 3rd Edition, TMH, 2011.
5. Patrick Engebretson, "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy", 2nd Edition, Elsevier, 2013.

ADDITIONAL REFERENCE BOOKS

1. Jon Erickson "HACKING: The art of Exploitation", 2nd Edition, William Pollock No Starch Press, 2008.

B.Tech. IV (CSE) Semester – VIII
CYBER LAW AND FORENSICS (CORE-16)
CS402

Scheme

L	T	P	Credit
3	0	2	04

1. <u>Course Outcomes (COs):</u> At the end of the course, students will be able to	
CO1	understand the basics of cyber law and cyber forensics with respect to Indian IT Act.
CO2	apply knowledge of cyber law to provide solutions to cyber security.
CO3	analyze various computer forensics technologies and systems.
CO4	evaluate and assess the methods for data recovery and digital evidence collection.
CO5	give solutions to real life problems using state of the art cyber forensics tools and techniques.

2. Syllabus

- **INTRODUCTION (08 Hours)**
Cyber Security and its Problem-Intervention Strategies: Redundancy, Diversity and Autarchy, Cyber-Crime and The Legal Landscape Around the World, Why Do We Need Cyber Laws, Cyber Forensics Fundamentals, Benefits of Forensics, Cyber Forensics Evidence and Courts, Legal Concerns and Private Issues.
- **CYBER LAWS -1 (08 Hours)**
The Indian IT Act, Challenges to Indian Law and Cybercrime Scenario in India, Consequences of Not Addressing the Weakness in Information Technology Act, Digital Signatures and the Indian IT Act, Cybercrime and Punishment, Cyber Law, Technology and Students: Indian Scenario.
- **CYBER LAWS -2 (08 Hours)**
Private Ordering Solutions, Regulation and Jurisdiction For Global Cyber Security, Copyright Source of Risks, Pirates, Internet Infringement, Fair Use, Postings, Criminal Liability, First Amendments, Data Losing, Cyber Ethics - Legal Developments, Cyber Security in Society, Security in Cyber Laws Case Studies, General Law and Cyber Law-A Swift Analysis.
- **CYBER FORENSICS -1 (09 Hours)**
Cyber Investigation - Procedure for Corporate High-Tech Investigations, Understanding Data Recovery Workstation and Software, Conducting and Investigations, Data Acquisition - Understanding Storage Formats and Digital Evidence, Determining the Best Acquisition Method, Acquisition Tools, Validating Data Acquisitions, Performing RAID Data Acquisitions, Remote Network Acquisition Tools, Other Forensics Acquisitions Tools.
- **CYBER FORENSICS -2 (09 Hours)**
Current Cyber Forensics Tools- Software and Hardware Tools, Validating and Testing Forensic Software, Addressing Data-Hiding Techniques, Performing Remote Acquisitions, E-Mail

Investigations- Investigating Email Crime and Violations, Understanding E-Mail Servers, Specialized E-Mail Forensics Tool.

- **Practicals will be based on the coverage of the above topics. (28 Hours)**
(Total Contact Time: 42 Hours + 28 Hours = 70 Hours)

3. Practicals:

- 1 Introduction to various software tools related to cyber law and cyber forensics.
- 2 Practical based on disk forensics.
- 3 Practical based on network forensics.
- 4 Practical based on device forensics.
- 5 Practical based on email security.
- 6 Practical using forensic tools for image and video fraud.
- 7 Practical using on e-commerce related cyber-attacks.
- 8 Practical based on social network and online transactions related cyber threats.

4. Books Recommended:

1. Sunit Belapure and Nina Godbole, Cyber "Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, 1st Edition, Wiley India Pvt. Ltd, 2011.
2. Mark F Grady, Francesco Parisi, "The Law and Economics of Cyber Security", 1st Edition, Cambridge University Press, 2006.
3. Jonathan Rosenoer, "Cyber Law: The law of the Internet", 1st Edition, Springer-Verlag, 1997.
4. Warren G. Kruse II and Jay G. Heiser, "Computer Forensics: Incident Response Essentials", 1st Edition, Addison Wesley, 2002.
5. B. Nelson, A. Phillips, F. Enfinger, C. Stuart, "Guide to Computer Forensics and Investigations, 2nd Edition, Thomson Course Technology, 2006, ISBN: 0-619-21706-5.

ADDITIONAL REFERENCE BOOKS

1. J. Vacca, "Computer Forensics: Computer Crime Scene Investigation", 2nd Edition, Charles River Media, 2005, ISBN: 1-58450-389.