CENTRAL UNIVERSITY OF PUNJAB
BATHINDA

M. Tech Computer Science & Technology
(Cyber Security)

Session - 2019-21

Department of Computer Science & Technology

SEMESTER-I

Course Code	Course Title	Course Type	Credit Hours		
			L	**T**	**P**
CBS.512	Advanced Data Structure and Algorithms	Core-I	4	0	0
CBS.513	Mathematical and Statistical Foundation of Computer Science	Core-II	4	0	0
CBS.506	Ethical Hacking	Elective-I	4	0	0
CBS.507	Intrusion Detection				
CBS.508	Data Encryption & Network Security	Elective-II	4	0	0
CBS.509	Information Theory				
CST.508	Machine Learning				
CST.514	Research Methodology	Foundation	4	0	0
XXX.YYY	Opt any one course from the courses offered by the University	IDC	2	0	0
CBS.515	Advanced Data Structure - Lab	Laboratory-I	0	0	2
CBS.510	Ethical Hacking- Lab	Laboratory-II	0	0	2
CBS.511	Intrusion Detection - Lab				
Total Credits			**22**	**0**	**4**

SEMESTER-II

Course Code	Course Title	Course Type	Credit Hours		
			L	T	P
CST.521	Advance Algorithm	Core-III	4	0	0
CST.522	Soft Computing	Core-IV	4	0	0
CBS.521	Malware Analysis & Reverse Engineering	Elective-III	4	0	0
CBS.522	Steganography				
CBS.523	Secure Software Design & Enterprise Computing				
CBS.524	Big Data Analysis and Visualization				
CST.524	IOT (Internet of Things)				
CBS.527	Digital Forensics	Elective-IV	4	0	0
CBS.525	Secure Coding				
CBS.526	Security Assessment & Risk Analysis				
CST.529	Blockchain Technology				
CBS.528	Python Programming for Security Professionals	Skill Development	4	0	0
XXX.YYY	Inter Disciplinary Course (IDC)	Audit Course	2	0	0
CST.527	Soft Computing-Lab	Laboratory-III	0	0	2
CBS.529	Python Programming for Security Professionals – Lab	Laboratory-IV	0	0	2
Total Credits			**22**	**0**	**4**

SEMESTER-III

Course Code	Course Title	Course Type	Credit Hours		
			L	T	P
CBS.551	Biometric Security	Discipline Elective	4	0	0
CST.552	Data Warehousing and Data Mining				
CST.553	Introduction to Intelligent System				
CST.554	Mobile Applications & Services				
CBS.552	Cyber Threat Intelligence	Open Elective	4	0	0
CST.556	Cost Management of Engineering Projects				
CBS.553	Cyber Law				
CST.557	Software Metrics				
XXX.YYY	Opt any one course from the courses offered by the University	Value Aided	2	0	0
CBS.559	Capstone Lab	Core	0	0	2
CBS.600	Dissertation/ Industrial Project	Core	0	0	10
Total Credits			**10**	**0**	**12**

*Students going for Industrial Project/ Thesis will complete these courses through MOOCs

SEMESTER-IV

Course Code	Course Title	Course Type	Credit Hours		
			L	T	P
CBS.600	Dissertation	Core	0	0	16
Total Credits			**0**	**0**	**16**

SEMESTER – I

Course Code: CBS.512
Course Title: Advanced Data Structures and Algorithms
Total Hours: 61

L	T	P	Cr
4	0	0	4

Course Objectives:

- Help students to understand and choose appropriate data structures for various algorithm designs.
- To familiarize students with advanced paradigms and algorithm analysis.
- Student should be able to come up with analysis of efficiency and proofs of correctness.

Learning Outcomes:

After completion of course, students would be able to:

- Explain the implementation of various data structures.
- Develop and analyze algorithms
- Identify suitable data structures and develop algorithms for computational geometry problems.

Unit I **14 Hours**

Algorithms and their complexity, Performance analysis: - Time and space complexity, asymptotic notation. Analyzing recursive algorithms using recurrence relations: Substitution method, Recursion tree method, Master method.

Divide and Conquer, and Greedy Algorithm Design Methodologies Introduction, Quick sort, Minimum spanning tree, Single source shortest path problem and their performance analysis.

Unit II **16 Hours**

Dynamic Programming and Backtracking Algorithm Design Methodologies Introduction, Traveling salesperson problem, Knapsack problem, multistage graphs, N-Queens problem.

Advanced Data Structures: Binary search trees, Red-Black Trees, B-trees, Fibonacci heaps, Data Structures for Disjoint Sets.

Dictionaries: Definition, Dictionary Abstract Data Type, Implementation of Dictionaries.

Hashing: Review of Hashing, Hash Function, Collision Resolution Techniques in Hashing, Separate Chaining, Open Addressing, Linear Probing, Quadratic Probing, Double Hashing, Rehashing, Extendible Hashing.

Unit III **16 Hours**

Advanced String Matching Algorithms Naïve string matching algorithm, Robin-Karp algorithm, string matching with finite automata, Knuth-Morris-Pratt algorithm.

Skip Lists: Need for Randomizing Data Structures and Algorithms, Search and Update Operations on Skip Lists, Probabilistic Analysis of Skip Lists, Deterministic Skip Lists.

Unit IV **15 Hours**

Graph Algorithms: Elementary graph algorithms, Minimum spanning trees, shortest path algorithms: single source and all pair.

Computational Geometry: One Dimensional Range Searching, Two Dimensional Range Searching, Constructing a Priority Search Tree, Searching a Priority Search Tree, Priority Range Trees, Quadtrees, k-D Trees.

Transactional Modes:

Lecture
Case study
Demonstration
Experimentation
Discussion
Problem solving

Suggested Readings:

1. Cormen, Leiserson, Rivest and Stein: Introduction to algorithms, Prentice-Hall of INDIA.
2. Horowitz, Sahni and Rajsekaran: Fundamentals of Computer Algorithms, Galgotia.
3. Aho, Hopcroft, Ullman: The Design and analysis of algorithms", Pearson Education
4. Sridhar, S., Design and Analysis of Algorithms. Oxford University Press India.
5. Mark Allen Weiss, Data Structures and Algorithm Analysis in C++, Pearson.
6. M T Goodrich, Roberto Tamassia, Algorithm Design, John Wiley.

Course Code: CBS.513

Course Title: Mathematical and Statistical Foundation of Computer Science

Total Hours: 64

L	T	P	Cr
4	0	0	4

Course Objectives:

To introduce students to mathematical and statistical fundamentals that is prerequisites for a variety of courses like Data mining, Network protocols, analysis of Web traffic, Computer security, Software engineering, Computer architecture, operating systems, distributed systems, Bioinformatics, Machine learning.

Course Outcomes:
After completion of course, students would be able to:

- To Identify and explain the basic notions of discrete and continuous probability.
- Describe the methods of statistical inference, and the role sampling distributions in these methods.
- To be able to select and implement correct and meaningful statistical analyses of simple to moderate complexity.

Unit I **17 hours**

Distribution Function: Probability mass, density. Cumulative distribution functions, Probability distributions (Binomial, Poisson and Normal). Expected value, Probabilistic inequalities, Random samples, sampling distributions of estimators Sampling distribution, Kurtosis and Skewness.

Unit II **15 hours**

Basic Statistics: Differences between parametric and non- parametric statistics, Univariant and multivariant analysis. Frequency distribution. Mean, Median, Mode, Probability Distribution, Standard deviation, Variation, Standard error, significance testing and levels of significance, One-way and two-way analysis of variance (ANOVA), Critical difference (CD). Introduction to Fuzzy Set Theory

Unit III **16 hours**

Statistical inference: Introduction to multivariate statistical models, Multivariate Regression, Multinominal regression and classification problems.
Graph Theory: Isomorphism, Planar graphs, graph colouring, Hamilton circuits and Euler cycles. Specialized techniques and Algorithms to solve combinatorial enumeration problems

Unit IV **16 hours**

Computer science and engineering applications with any of following area: Data mining, Computer security, Software engineering, Computer architecture, Bioinformatics, Machine learning. Recent Trends in various distribution functions in mathematical field of computer science for varying fields like, soft computing, and computer vision.

Transactional Modes:
Lecture
Case study
Demonstration
Experimentation
Discussion
Problem solving

Suggested Readings:

1. John Vince, Foundation Mathematics for Computer Science, Springer International Publishing.
2. Kishor S. Trivedi, Probability and Statistics with Reliability, Queuing, and Computer Science Applications.
3. Michel Mitzenmacher and E. Upfal. Probability and Computing: Randomized Algorithms and Probabilistic Analysis, Cambrige University Press.
4. Alan Tucker, Applied Combinatorics, Wiley.

Course Code: CBS.506
Course Title: Ethical Hacking
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:

The objective of this course is:

- To introduces the concepts of Ethical Hacking.
- Gives the students the opportunity to learn about different tools and techniques in Ethical hacking and security.
- Practically apply Ethical hacking tools to perform various activities.

Learning Outcomes:

After completion of course, students would be able to:

- Explain the core concepts related to vulnerabilities and their causes.
- Discuss ethics behind hacking and vulnerability disclosure.
- Demonstrate the impact of hacking.
- Design methods to extract vulnerabilities related to computer system and networks using state of the art tools and technologies.

Unit I **13 Hours**

Ethical hacking process, Hackers behaviour & mindset, Maintaining Anonymity, Hacking Methodology, Information Gathering, Active and Passive Sniffing, Physical security vulnerabilities and countermeasures. Internal and External testing. Preparation of Ethical Hacking and Penetration Test Reports and Documents.

Unit II **17 Hours**

Social Engineering attacks and countermeasures. Password attacks, Privilege Escalation and Executing Applications, Network Infrastructure Vulnerabilities, IP spoofing, DNS spoofing.

Wireless Hacking: Wireless footprint, Wireless scanning and enumeration, Gaining access, (hacking 802.11), WEP, WPA, WPA2.

Unit III **14 Hours**

DoS attacks. Web server and application vulnerabilities, SQL injection attacks, Vulnerability Analysis and Reverse Engineering, Buffer overflow attacks. Client-side browser exploits, Exploiting Windows Access Control Model for Local Elevation Privilege. Exploiting vulnerabilities in Mobile Application.

Unit IV **16 Hours**

Introduction to Metasploit: Metasploit framework, Metasploit Console, Payloads, Metrpreter, Introduction to Armitage, Installing and using Kali Linux Distribution, Introduction to penetration testing tools in Kali Linux. Case Studies of recent vulnerabilities and attacks.

Transactional Modes:

Lecture	Experimentation
Case study	Discussion
Demonstration	Problem solving

Suggested Readings:

1. Baloch, R., Ethical Hacking and Penetration Testing Guide, CRC Press.
2. Dafydd Stuttard, Marcus Pinto, The Web Application Hacker's Handbook, Wiley.
3. Beaver, K., Hacking for Dummies, John Wiley & sons.
4. Council, Ec. , Computer Forensics: Investigating Network Intrusions and Cybercrime, Cengage Learning.
5. McClure S., Scambray J., and Kurtz G, Hacking Exposed. Tata McGraw-Hill Education.
6. International Council of E-Commerce Consultants by Learning, Penetration Testing Network and Perimeter Testing Ec-Council/ Certified Security Analyst Vol. 3 of Penetration Testing, Cenage Learning.
7. Davidoff, S. and Ham, J., Network Forensics Tracking Hackers through Cyberspace, Prentice Hall.
8. Michael G. Solomon, K Rudolph, Ed Tittel, Broom N., and Barrett, D.,Computer, Forensics Jump Start, Willey Publishing.

Code: CBS.507
Course Title: Intrusion Detection
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:

The objective of this course is to:

- Compare alternative tools and approaches for Intrusion Detection through quantitative analysis to determine the best tool or approach to reduce risk from intrusion.

- Identify and describe the parts of all intrusion detection systems and characterize new and emerging IDS technologies according to the basic capabilities all intrusion detection systems share.

Learning Outcomes:

After completion of course, students would be able to:

- Apply knowledge of the fundamentals and history of Intrusion Detection in order to avoid common pitfalls in the creation and evaluation of new Intrusion Detection Systems.
- Evaluate the security of an enterprise and appropriately apply Intrusion Detection tools and techniques in order to improve their security posture.

UNIT I **12 Hours**

The state of threats against computers, and networked Systems-Overview of computer security solutions and why they Fail-Vulnerability assessment, firewalls, VPN's –Overview of Intrusion Detection and Intrusion Prevention-Network and Host-based IDS.

UNIT II **14 Hours**

Classes of attacks – Network layer: scans, denial of service, penetration – Application layer: software exploits, code Injection-Human layer: identity theft, root access-Classes of attackers-Kids/hackers/sop Hesitated groups-Automated: Drones, Worms, Viruses.

UNIT III **16 Hours**

A General IDS model and taxonomy, Signature-based Solutions, Snort, Snort rules, Evaluation of IDS, Cost sensitive IDS Anomaly Detection Systems and Algorithms-Network Behavior Based Anomaly Detectors (rate based)-Host-based Anomaly Detectors-Software Vulnerabilities- State transition, Immunology, Payload Anomaly Detection.

UNIT IV **18 Hours**

Attack trees and Correlation of Alerts-Autopsy of Worms and Botnets-Malware Detection-Obfuscation, Polymorphism-Document vectors. Email/IM security Issues-Viruses/Spam-From signatures to thumbprints to zero day. Detection-Insider Threat Issues-Taxonomy-Masquerade and Impersonation-Traitors, Decoys and Deception-Future: Collaborative Security.

Transactional Modes:

Lecture	Experimentation
Case study	Discussion
Demonstration	Problem solving

Suggested Readings:

1. Peter Szor, The Art of Computer Virus Research and Defense, Symantec Press.

2. Markus Jakobsson and Zulfikar Ramzan, Crimeware, Understanding New Attacks and Defenses, Symantec Press.

Code: CBS.508
Course Title: Data Encryption & Network Security
Total Hours: 56

L	T	P	Cr
4	0	0	4

Course Objectives:
The objective of this course is to:

- To introduce students to the concept of security, and types of attacks.
- Describe Symmetric & Asymmetric Key Cryptography
- Define Network Perimeter Security, Access Control Lists and Virtual Private Networks.

Learning Outcomes:
After completion of course, students would be able to:

- Identify the domain specific security issues.
- Apply Symmetric & Asymmetric Key Cryptography in various applications.
- Design Access Control Lists and Virtual Private Networks.

UNIT I **10 Hours**

Introduction to Security: Need for security, Security approaches, Principles of security, Types of attacks.
Encryption Techniques: Plaintext, Cipher text, Substitution & Transposition Techniques, Encryption & Decryption, Types of attacks, Key range & Size.

UNIT II **15 Hours**

Symmetric & Asymmetric Key Cryptography: Algorithm types & Modes, DES, IDEA, Differential & Linear Cryptanalysis, Knapsack algorithm, Public-Key Cryptography Principles, RSA, Symmetric & Asymmetric key together.
User Authentication Mechanism: Authentication basics, Passwords, Authentication tokens, Certificate based & Biometric authentication.

UNIT III **16 Hours**

Case Studies of Cryptography: Denial of service attacks, IP spoofing attacks, Secure inter branch payment transactions, Conventional Encryption and Message Confidentiality, Conventional Encryption Principles, Conventional Encryption Algorithms, Location of Encryption Devices, Key Distribution.
Message Authentication**:** Approaches to Message Authentication, SHA-1, MD5, Digital, Signatures, Key Management.

UNIT IV **15 Hours**

Network Perimeter Security Fundamentals: Introduction to Network Perimeter, Multiple layers of Network Security, Security by Router.
Firewalls: Firewall Basics, Types of Firewalls, Network Address Translation Issues.

Access Control Lists: Ingress and Egress Filtering, Types of Access Control Lists, ACL types: standard and extended, ACL commands.
Virtual Private Networks: VPN Basics, Types of VPN, IPsec Tunneling, IPsec Protocols.
VLAN: introduction to VLAN, VLAN Links, VLAN Tagging, VLAN Trunk Protocol (VTP).

Transactional Modes:
Lecture
Case study
Demonstration
Experimentation
Discussion
Problem solving

Suggested Readings:

1. Forouzan, B.A., Cryptography & Network Security. Tata McGraw-Hill Education.
2. Kahate, A. Cryptography and Network Security. McGraw-Hill Higher Ed.
3. Godbole, N., Information Systems Security: Security Management, Metrics, Frameworks and Best Practices. John Wiley & Sons India.
4. Riggs, C., Network Perimeter Security: Building Defence In-Depth, AUERBACH, USA.
5. Northcutt S., Inside Network Perimeter Security, Pearson Education.
6. Stallings, W., Network Security Essentials: applications and standards. Pearson Education India.
7. Stallings, W., Cryptography and Network Security: Principles and Practice. Pearson.
8. Kim. D., and Solution, M.G., Fundamentals of Information System Security. Jones & Bartlett Learning.

Code: CBS.509
Course Title: Information Theory
Total Hours: 59

L	T	P	Cr
4	0	0	4

Course Objectives:
- The course provides an insight to information theory.
- Help to familiarize the students with coding techniques and error correction mechanism.
- Give student opportunity to compare and contrast various coding techniques

Learning Outcomes:
After completion of course, students would be able to:
- Describe the principles and applications of information theory.

- Demonstrate how information is measured in terms of probability and entropy.
- Compare coding schemes, including error correcting codes.

UNIT I **16 Hours**

Information and entropy information measures, Shannon's concept of Information. Channel coding, channel mutual information capacity (BW). Theorem for discrete memory less channel, information capacity theorem, Error detecting and error correcting codes.

UNIT II **14 Hours**

Types of codes: block codes, Hamming and Lee metrics, description of linear block codes, parity check Codes, cyclic code, Masking techniques.

UNIT III **13 Hours**

Compression: loss less and lossy, Huffman codes, LZW algorithm, Binary Image c compression schemes, run length encoding, CCITT group 3 1- D Compression, CCITT group 3 2D compression, CCITT group 4 2DCompression.

UNIT IV **16 Hours**

Convolutional codes, sequential decoding. Video image Compression: CITT H 261 Video coding algorithm, audio (speech) Compression. Cryptography and cipher.

Case study of CCITT group 3 1-DCompression, CCITT group 3 2D compression. Case Study of Advanced compression technique and Audio compression.

Transactional Modes:

Lecture	Experimentation
Case study	Discussion
Demonstration	Problem solving

Suggested Readings:

1. Monica Borda, Fundamentals in information theory and coding, Springer.
2. Singh and Sapre, Communication Systems: Analog and digital, Tata McGraw Hill.
3. Fred Halsall, Multimedia Communications, Addition-Wesley.
4. Ranjan Bose, Information Theory, Coding and Cryptography, Tata McGraw Hill.
5. Prabhat K Andleigh and Kiran Thakrar, Multimedia system Design, Prentice Hall PTR.

Course Code: CST.508
Course Title: Machine Learning
Total Hours: 63

L	T	P	Cr
4	0	0	4

Course Objectives:
The objective of this course is to:

- To help students learn the concept of how to learn patterns and concepts from data without being explicitly programmed in various IOT nodes.
- To design and analyze various machine learning algorithms and techniques with a modern outlook focusing on recent advances.
- Explore supervised and unsupervised learning paradigms of machine learning.
- To explore ANN and Deep learning technique and various feature extraction strategies.

Learning Outcomes:
After completion of course, students would be able to:

- Extract features that can be used for a particular machine learning approach in various IOT applications.
- To compare and contrast pros and cons of various machine learning techniques and to get an insight of when to apply a particular machine learning approach.
- To mathematically analyze various machine learning approaches and paradigms.

UNIT I **16 Hours**

Introduction to learning Techniques: Supervised Learning (Regression/Classification)

- Basic methods: Distance-based methods, Nearest-Neighbours, Decision Trees, Naive Bayes
- Linear models: Linear Regression, Logistic Regression, Generalized Linear Models
- Support Vector Machines, Nonlinearity and Kernel Methods
- Beyond Binary Classification: Multi-class/Structured Outputs, Ranking

UNIT II **15 Hours**

Unsupervised Learning

- Clustering: K-means/Kernel K-means
- Dimensionality Reduction: PCA and kernel PCA
- Matrix Factorization and Matrix Completion
- Generative Models (mixture models and latent factor models)

UNIT III **14 Hours**

Evaluating Machine Learning algorithms and Model Selection, Introduction to Statistical Learning Theory, Ensemble Methods (Boosting, Bagging, Random Forests).

Sparse Modeling and Estimation, Modeling Sequence/Time-Series Data, Deep Learning and Feature Representation Learning.

Introduction to ANN and Deep learning.

UNIT IV **18 Hours**

Scalable Machine Learning (Online and Distributed Learning) A selection from some other advanced topics, e.g., Semi-supervised Learning, Active Learning, Reinforcement Learning, Inference in Graphical Models, Introduction to Bayesian Learning and Inference.

Simulation Tool for Machine Learning, Hands on with recent tools WEKA, R, MATLAB

Recent trends in various learning techniques of machine learning and classification methods for IOT applications. Various models for IOT applications.

Transactional Modes:

Lecture
Case study
Demonstration
Experimentation
Discussion
Problem solving

Suggested Readings:

1. Kevin Murphy, Machine Learning: A Probabilistic Perspective, MIT Press.
2. Trevor Hastie, Robert Tibshirani, Jerome Friedman, The Elements of Statistical Learning, Springer. (freely available online)
3. Christopher Bishop, Pattern Recognition and Machine Learning, Springer.
4. Shai Shalev-Shwartz, Shai Ben-David, Understanding Machine Learning: From Theory to Algorithms, Cambridge University Press.

Code: CST. 514
Course Title: Research Methodology
Total Hours: 59

L	T	P	Cr
4	0	0	4

Course Objectives:

- To develop a research orientation among the students and help them understand fundamentals of research methods.
- The course will help the students to identify various sources of information for literature review, data collection and effective paper/ dissertation writing.
- Familiarize students with the concept of patents and copyright

Learning Outcomes:
After completion of course, students would be able to:

- Enable the students to effectively formulate a research problem.
- Analyze research related information and follow research ethics.
- Apply intellectual property law principles (including copyright, patents, designs and trademarks) to practical problems and be able to analyse the social impact of IPR.

UNIT I **14 Hours**

Meaning of research problem, Sources of research problem, Criteria Characteristics of a good research problem, Errors in selecting a research problem, Scope and objectives of research problem. Approaches of investigation of solutions for research problem, data collection, analysis, interpretation, Necessary instrumentations.

UNIT II **15 Hours**

Effective literature studies approaches, analysis Plagiarism, Research ethics, Effective technical writing, how to write report, Paper
Developing a Research Proposal, Format of research proposal, a presentation and assessment by a review committee.

UNIT III **14 Hours**

Nature of Intellectual Property: Patents, Designs, Trade and Copyright. Process of Patenting and Development: technological research, innovation, patenting, development.
International Scenario: International cooperation on Intellectual Property. Procedure for grants of patents, Patenting under PCT.

UNIT IV **16 Hours**

Patent Rights: Scope of Patent Rights. Licensing and transfer of technology. Patent information and databases. Geographical Indications.
New Developments in IPR: Administration of Patent System. New developments in IPR; IPR of Biological Systems, Computer Software, Integrated Circuits, etc.

Transactional Modes:
Lecture
Case study
Demonstration
Experimentation
Discussion
Problem solving

Suggested Readings:

1. Stuart Melville and Wayne Goddard, Research methodology: an introduction for science & engineering students, Juta Academic.
2. Wayne Goddard and Stuart Melville, Research Methodology: An Introduction, Juta Academic.

3. Ranjit Kumar, Research Methodology: A Step by Step Guide for beginners, SAGE Publications Ltd.
4. Halbert, Resisting Intellectual Property, Taylor & Francis Ltd.
5. Mayall , Industrial Design, McGraw Hill.
6. Niebel , Product Design, McGraw Hill.
7. Asimov, Introduction to Design, Prentice Hall.
8. Robert P. Merges, Peter S. Menell, Mark A. Lemley, Intellectual Property in New Technological Age.

Code: CBS.515
Course Title: Advanced Data Structure -Lab

L	T	P	Cr
0	0	4	2

Course Objectives:

- Develop skills to design and analyse simple linear and non-linear data structures.
- Strengthen the ability to identify and apply the suitable data structure for implementation of a specific algorithm.
- Gain knowledge in practical implementation of data structures and algorithms.

Learning Outcomes:
After completion of course, students would be able to:

- Be able to design and analyse different data structures·
- Be capable to identify the appropriate data structure for a given algorithm.
- Implement various data structures and algorithms.

Lab Assignments will be based on topics studied in Subject

Lab Evaluation:
The criteria for evaluation of lab will be based on following parameters:

Component	**Marks**
Continuous Evaluation	30
End Term (Implementation and Viva-Voce)	20
Total	**50**

Code: CBS.510
Course Title: Ethical Hacking Lab

L	T	P	Cr
0	0	4	2

Course Objective:
The objective of this course is:

- The objective of this course is to enable the students to explore the tools required to perform penetration testing.
- Gain a fundamental understanding of ethical hacking process by performing a variety of tasks required to perform testing of Computer System, Web application and network.

Learning Outcomes:
Upon successfully completing this course, students will be able to:

- Select appropriate tool for various activities related to ethical hacking
- Design an ethical hacking plan
- Identify various vulnerabilities
- Write test reports

List of Practical will be based on Elective – I subject opted by the students

Lab Evaluation:
The criteria for evaluation of lab will be based on following parameters:

Component	**Marks**
Continuous Evaluation	30
End Term (Implementation and Viva-Voce)	20
Total	**50**

Code: CBS.511
Course Title: Intrusion Detection Lab

L	**T**	**P**	**Cr**
0	0	4	2

Course Objectives:
The objective of this course is to:

- To compare alternative tools and approaches for Intrusion Detection.
- To determine the best tool or approach to reduce risk from intrusion.
- To identify and describe the parts of all intrusion detection systems
- To illustrate new and emerging IDS technologies.

Course Outcomes:
After completion of course, students would be able to:

- Apply knowledge of the fundamentals of Intrusion Detection in order to avoid common pitfalls in the creation and
- Implement new Intrusion Detection Systems.
- Evaluate Intrusion Detection tools and techniques in order to improve their security posture.

List of Practical will be based on Elective – I subject opted by the students

Lab Evaluation:
The criteria for evaluation of lab will be based on following parameters:

Component	**Marks**
Continuous Evaluation	30
End Term (Implementation and Viva-Voce)	20
Total	**50**

Code: CST.517
Course Title: Machine Learning Lab

L	T	P	Cr
0	0	4	2

Course Objectives:

- The objectives of the Machine Learning Lab are to introduce students to the basic concepts and techniques of Machine Learning.
- To develop skills of using recent machine learning software for solving practical problems.

Learning Outcomes:
After completion of course, students would be able to:

- Understand some common Machine Learning algorithms and their limitations.
- Apply common Machine Learning algorithms in practice and implementing the same.
- Perform experiments in Machine Learning using real-world data.

List of Practical will be based on Elective – I subject opted by the students

Lab Evaluation:

The criteria for evaluation of lab will be based on following parameters:

Component	**Marks**
Continuous Evaluation	30
End Term (Implementation and Viva-Voce)	20
Total	**50**

SEMESTER -II

Code: CST. 521
Course Title: Advance Algorithm
Total Hours: 61

L	T	P	Cr
4	0	0	4

Course Objectives:
The objective of this course is to:

- To familiarize students with basic paradigms and data structures used to solve advanced algorithmic problems
- To introduce the students to recent developments in the area of algorithmic design.

Learning Outcomes:
After completion of course, students would be able to:

- Analyze the complexity/performance of different algorithms.
- Determine the appropriate data structure for solving a particular set of problems.

- Categorize the different problems in various classes according to their complexity.

UNIT I **16 Hours**

Sorting: Review of various sorting algorithms, topological sorting
Graph: Definitions and Elementary Algorithms: Shortest path by BFS, shortest path in edge-weighted case (Dijkasra's), depth-first search and computation of strongly connected components, Emphasis on correctness proof of the algorithm and time/space analysis, Introduction to greedy paradigm, algorithm to compute a maximum weight maximal independent set. Application to MST.

UNIT II **14 Hours**

Strassen's algorithm and introduction to divide and conquer paradigm, inverse of a triangular matrix, relation between the time complexities of basic matrix operations.
Floyd-Warshall algorithm and introduction to dynamic programming paradigm. More examples of dynamic programming.

UNIT III **15 Hours**

Linear Programming: Geometry of the feasibility region and Simplex algorithm, Decision Problems: P, NP, NP Complete, NP-Hard, NP Hard with Examples, Proof of NP-hardness and NP-completeness.

UNIT IV **16 Hours**

One or more of the following topics based on time and interest Approximation algorithms, Randomized Algorithms, Interior Point Method, Recent Trends in problem solving paradigms using recent searching and sorting techniques by applying recently proposed data structures.

Transactional Modes:

Lecture
Case study
Demonstration
Experimentation
Discussion
Problem solving

Suggested Readings:

1. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest Introduction to Algorithms, Stein.
2. Alfred V. Aho, John E. Hopcroft, Jeffrey D. Ullman, The Design and Analysis of Computer Algorithms.
3. Jon Kleinberg and Eva Tardos , Algorithm Design.
4. Juraj Hromkovic, Design and Analysis of Randomized Algorithms: Introduction to Design.

Code: CST. 522
Course Title: Soft Computing
Total Hours: 58

L	T	P	Cr
4	0	0	4

Course Objectives:

- To introduce soft computing concepts and techniques and foster their abilities in designing appropriate technique for a given scenario.
- To give students knowledge of non-traditional technologies and fundamentals of artificial neural networks, fuzzy sets, fuzzy logic, genetic algorithms.
- To provide student hand-on experience to implement various strategies.

Learning Outcomes:

After completion of course, students would be able to:

- Identify and describe soft computing techniques and their roles in building intelligent machines.
- Apply fuzzy logic and reasoning to handle uncertainty and solve various engineering problems.
- Apply genetic algorithms to combinatorial optimization problems.
- Evaluate and compare solutions by various soft computing approaches for a given problem.

UNIT I **14 Hours**

Introduction to Soft Computing and Neural Networks: Evolution of Computing: Soft Computing Constituents, From Conventional AI to Computational Intelligence: Machine Learning Basics. Adaptive Resonance architectures, Advances in Neural networks.

Neural Networks: Machine Learning Using Neural Network, Adaptive Networks, Feed forward Networks, Supervised Learning Neural Networks, Radial Basis Function Networks: Reinforcement Learning, Unsupervised Learning Neural Networks.

UNIT II **14 Hours**

Fuzzy Logic: Fuzzy Sets, Membership Functions, Operations on Fuzzy Sets, Fuzzy Relations.

Fuzzy Rules and Fuzzy Reasoning, Fuzzy Inference Systems, Fuzzy Expert Systems, Fuzzy Decision Making, Fuzzy Models.

UNIT III **16 Hours**

Genetic Algorithms: Introduction to Genetic Algorithms (GA), Applications of GA in Machine Learning: Machine Learning Approach to Knowledge Acquisition. Introduction to other optimization techniques.

UNIT IV **14 Hours**

Implementation of simple artificial neural networks, fuzzy logic techniques and genetic algorithms.

Recent trends in soft computing techniques. Introduction to hybrid systems and swarm intelligence.

Transactional Modes:
Lecture
Case study
Demonstration
Experimentation
Discussion
Problem solving

Suggested Readings:

1. Jyh-Shing Roger Jang, Chuen-Tsai Sun, Eiji Mizutani, Neuro - Fuzzy and Soft Computing, Prentice-Hall of India.
2. George J. Klir and Bo Yuan, Fuzzy Sets and Fuzzy Logic - Theory and Applications, Prentice Hall.
3. Ross J.T., Fuzzy Logic with Engineering Applications John Wiley & Sons.
4. Rajasekaran, S. Vijayalakshmi Pai, G.A. Neural Networks, Fuzzy Logic and Genetic Algorithms PHI Learning.
5. Priddy L.K., Keller E.P., Artificial Neural Networks: An Introduction, SPIE Press.
6. Gen, M. Cheng R., Genetic Algorithms and Engineering Optimization John Wiley & Sons.

Code: CBS. 521
Course Title: Malware Analysis & Reverse Engineering
Total Hours: 66

L	T	P	Cr
4	0	0	4

Course Objectives:
The objective of this course is to provide an insight to fundamentals of malware analysis which includes analysis of JIT compilers for malware detection in legitimate code. DNS filtering and reverse engineering is included.

Learning Outcomes:
After completion of course, students would be able to:
- To understand the concept of malware and reverse engineering.
- Implement tools and techniques of malware analysis.

UNIT I **18 Hours**
Fundamentals of Malware Analysis (MA), Reverse Engineering Malware (REM) Methodology, Brief Overview of Malware analysis lab setup and configuration, Introduction to key MA tools and techniques, Behavioral Analysis vs. Code Analysis, Resources for Reverse-Engineering Malware (REM) Understanding Malware Threats, Malware indicators, Malware Classification, Examining Clam AV Signatures, Creating Custom Clam AV Databases, Using YARA to Detect Malware Capabilities, Creating a

Controlled and Isolated Laboratory, Introduction to MA Sandboxes, Ubuntu, Zeltser's REMnux, SANS SIFT, Sandbox Setup and Configuration New Course Form, Routing TCP/IP Connections, Capturing and Analyzing Network Traffic, Internet simulation using INetSim, Using Deep Freeze to Preserve Physical Systems, Using FOG for Cloning and Imaging Disks, Using MySQL Database to Automate FOG Tasks.

UNIT II **15 Hours**

Introduction to Python, Introduction to x86 Intel assembly language, Scanners: Virus Total, Jotti, and NoVirus Thanks, Analyzers: Threat Expert, CWSandbox, Anubis, Joebox, Dynamic Analysis Tools: Process Monitor, Regshot, HandleDiff, Analysis Automation Tools: Virtual Box, VM Ware, Python , Other Analysis Tools.

Malware Forensics

Using TSK for Network and Host Discoveries, Using Microsoft Offline API to Registry Discoveries , Identifying Packers using PEiD, Registry Forensics with Reg Ripper Plu-gins:, Bypassing Poison Ivy's Locked Files, Bypassing Conficker's File System ACL Restrictions, Detecting Rogue PKI Certificates.

UNIT III **16 Hours**

Malware and Kernel Debugging

Opening and Attaching to Processes, Configuration of JIT Debugger for Shellcode Analysis, Controlling Program Execution, Setting and Catching Breakpoints, Debugging with Python Scripts and Py Commands**,** DLL Export Enumeration, Execution, and Debugging**,** Debugging a VMware Workstation Guest (on Windows)**,** Debugging a Parallels Guest (on Mac OS X). Introduction to WinDbg Commands and Controls, Detecting Rootkits with WinDbgScripts**,** Kernel Debugging with IDA Pro.

UNIT IV **17 Hours**

Memory Forensics and Volatility

Memory Dumping with MoonSols Windows Memory Toolkit, Accessing VM Memory Files Overview of Volatility, Investigating Processes in Memory Dumps**,** Code Injection and Extraction**,** Detecting and Capturing Suspicious Loaded DLLs**,** Finding Artifacts in Process Memory**,** Identifying Injected Code with Malfind and YARA.

Using WHOIS to Research Domains**,** DNS Hostname Resolution**,** Querying, Passive DNS**,** Checking DNS Records**,** Reverse IP Search New Course Form**,** Creating Static Maps**,** Creating Interactive Maps.

Case study of Finding Artifacts in Process Memory, Identifying Injected Code with Malfind and YARA.

Transactional Modes:

Lecture
Case study
Demonstration
Experimentation
Discussion
Problem solving

Suggested Readings:

1. Michael Sikorski, Andrew Honig, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software publisher William Pollock.
2. Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory.

Code: CBS.522
Course Title: Steganography
Total Hours: 57

L	T	P	Cr
4	0	0	4

Course Objectives:

The objective of course is to provide an insight to steganography techniques. Watermarking techniques along with attacks on data hiding and integrity of data is included in this course.

Learning Outcomes:

After completion of course, students would be able to:

- Describe the concept of information hiding.
- Examine the current techniques of steganography and learn how to detect and extract hidden information.
- Classify and apply watermarking techniques.

UNIT I **14 Hours**

Steganography: Overview, History, Methods for hiding (text, images, audio, video, speech etc.), Issues: Security, Capacity and Imperceptibility, Steganalysis: Active and Malicious Attackers, Active and passive steganalysis.

UNIT II **12 Hours**

Frameworks for secret communication (pure Steganography, secret key, public key steganography), Steganography algorithms (adaptive and non-adaptive).

UNIT III **15 Hours**

Steganography techniques: Substitution systems, Spatial Domain, Transform domain techniques, Spread spectrum, Statistical steganography, Cover Generation and cover selection, Tools: EzStego, FFEncode, Hide 4 PGP, Hide and Seek, S Tools etc.)

Detection, Distortion, Techniques: LSB Embedding, LSB Steganalysis using primary sets, Texture based.).

UNIT IV **16 Hours**

Digital Watermarking: Introduction, Difference between Watermarking and Steganography, History, Classification (Characteristics and Applications), Types and techniques (Spatial-domain, Frequency-domain, and Vector quantization based watermarking), Attacks and Tools (Attacks by Filtering,

Remodulation, Distortion, Geometric Compression, Linear Compression etc.), Watermark security & authentication.
Recent trends in Steganography and digital watermarking techniques. Case study of LSB Embedding, LSB Steganalysis using primary sets.

Transactional Modes:
Lecture
Case study
Demonstration
Experimentation
Discussion
Problem solving

Suggested Readings:

1. Peter Wayner, Disappearing Cryptography–Information Hiding: Steganography & Watermarking, Morgan Kaufmann Publishers, New York.
2. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, TonKalker, Digital Watermarking and Steganography, Margan Kaufmann Publishers, New York.
3. Neil F. Johnson, Zoran Duric, Sushil Jajodia, Information Hiding: Steganography and Watermarking-Attacks and Countermeasures, Springer.
4. Stefan Katzenbeisser, Fabien A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House Print on Demand.

Code: CBS.523
Course Title: Secure Software Design and Enterprise Computing
Total Hours: 57

L	T	P	Cr
4	0	0	4

Course Objectives:
The objective of this course is to:
- To make students aware of various issues like weak random number generation, information leakage, poor usability, and weak or no encryption on data traffic.
- Techniques for successfully implementing and supporting network services on an enterprise scale and heterogeneous systems environment.
- Methodologies and tools to design and develop secure software containing minimum vulnerabilities and flaws.

Learning Outcomes:
After completion of course, students would be able to:
- Differentiate between various software vulnerabilities.
- Process vulnerabilities for an organization.
- Monitor resources consumption in a software.
- Interrelate security and software development process.

UNIT I **13 Hours**

Secure Software Design

Identify software vulnerabilities and perform software security analysis, Master security programming practices, Master fundamental software security design concepts, Perform security testing and quality assurance.

UNIT II **15 Hours**

Enterprise Application Development

Describe the nature and scope of enterprise software applications, Design distributed N-tier software application, Research technologies available for the presentation, business and data tiers of an enterprise software application, Design and build a database using an enterprise database system, Develop components at the different tiers in an enterprise system, Design and develop a multi-tier solution to a problem using technologies used in enterprise system, Present software solution.

UNIT III **16 Hours**

Enterprise Systems Administration

Design, implement and maintain a directory-based server infrastructure in a heterogeneous systems environment, Monitor server resource utilization for system reliability and availability, Install and administer network services (DNS/DHCP/Terminal Services/Clustering/Web/Email).

UNIT IV **16 Hours**

Obtain the ability to manage and troubleshoot a network running multiple services, Understand the requirements of an enterprise network and how to go about managing them.

Handle insecure exceptions and command/SQL injection, Defend web and mobile applications against attackers, software containing minimum Vulnerabilities and flaws.

Case study of DNS server, DHCP configuration and SQL injection attack.

Transactional Modes:

Lecture
Case study
Demonstration
Experimentation
Discussion
Problem solving

Suggested Readings:

1. Theodor Richardson, Charles N Thies, Secure Software Design, Jones & Bartlett.
2. Kenneth R. van Wyk, Mark G. Graff, Dan S. Peters, Diana L. Burley, Enterprise Software Security, Addison Wesley.

Code: CBS.524
Course Title: Big Data Analysis and Visualization
Total Hours: 61

L	T	P	Cr
4	0	0	4

Course Objectives:
The objective of this course is to:

- To prepare the Big Data for analysis.
- To extract the meaningful data from unstructured Big Data and develop Data Visualizations skill.
- To apply various tools for analysis of structured and unstructured Big Data.

Learning Outcomes:
After completion of course, students would be able to:

- Analyse the identification of Big Data problem
- Extract the structured data from unstructured data.
- Use Hadoop related tools such as JAQL, Spark, Pig and Hive for structured and unstructured Big Data analytics

UNIT I **15 Hours**

Big Data Introduction: What is big data, why big data, convergence of key trends, unstructured data, industry examples of big data, web analytics, big data and marketing, fraud and big data, risk and big data, big data and healthcare, big data in medicine, advertising and big data, big data technologies, open source technologies, cloud and big data, mobile business intelligence, Crowd sourcing analytics, inter and trans firewall analytics.
Data Gathering and Preparation: Data formats, parsing and transformation, Scalability and real-time issues.

UNIT II **16 Hours**

Data Cleaning: Consistency checking, Heterogeneous and missing data, Data Transformation and segmentation.
Visualization: Descriptive and comparative statistics, Designing visualizations, Time series, Geo-located data, Correlations and connections, Hierarchies and networks, interactivity.

UNIT III **15 Hours**

Big Data Technology: Big Data Architecture, Big Data Warehouse, Functional Vs. Procedural Programming Models for Big Data
NoSQL: Introduction to NoSQL, aggregate data models, key-value and document data models.

UNIT IV **15 Hours**

Big Data Tools: Hadoop: Introduction to Hadoop Ecosystem, HDFS, Map-Reduce programming, Spark, PIG, JAQL, Understanding Text Analytics and Big Data, Predictive Analysis of Big Data, Role of Data Analyst.

Transactional Modes:
Lecture
Case study
Demonstration
Experimentation
Discussion
Problem solving

Suggested Readings:

1. EMC Education Services, Data Science and Big Data Analytics: Discovering, Analyzing, Visualizing and Presenting Data | IM | BS , John WIley & Sons.
2. Anil Maheshwari, Data Analytics Make Accesible, Orilley Publications.
3. Croll and B. Yoskovitz Lean Analytics: Use Data to Build a Better Startup Faster, Oreilley Publications.

Code: CST.524
Course Title: IOT (Internet of Things)
Total Hours: 54

L	T	P	Cr
4	0	0	4

Course Objectives:
The objective of this course is to:
- The objective of this course is to introduce students to the concepts of Internet of Things
- Help the students learn to use of devices in IoT Technology,
- Identify Real World IoT Design Constraints.

Learning Outcomes:
After completion of course, students would be able to:
- Describe the domain specific applications
- Analyze the challenges in IoT Design
- Design IoT applications on different embedded platform.

UNIT I **10 Hours**
Introduction to IoT: Defining IoT, Characteristics of IoT, Physical design of IoT, Logical design of IoT, Functional blocks of IoT, Communication models and APIs IoT and M2M, Difference between IoT and M2M, Software define Network.

UNIT II **12 Hours**
Network and Communication aspects: Wireless medium access issues, MAC protocol survey, Survey routing protocols, Sensor deployment, Node discovery, Data aggregation and Dissemination.

UNIT III **16 Hours**
Challenges in IoT Design: challenges, Development challenges, Security challenges, Other Challenges

Domain specific applications: IoT Home automation, Industry applications, Surveillance applications, Other IoT applications

UNIT IV **16 Hours**

Developing IoTs: Developing applications through IoT tools including Python/Arduino/Raspberry pi, Developing sensor based application through embedded system platform.

Transactional Modes:

Lecture
Case study
Demonstration
Experimentation
Discussion
Problem solving

Suggested Readings:

1. Vijay Madisetti, Arshdeep Bahga, Internet of Things: A Hands-On Approach, Orient Blackswan Pvt. Ltd.- New Delhi.
2. Waltenegus Dargie, Christian Poellabauer, Fundamentals of Wireless Sensor Networks: Theory and Practice, Wiley-Blackwell.
3. Francis da Costa, Rethinking the Internet of Things: A Scalable Approach to Connecting Everything, Apress Publications.
4. Jan Holler, Vlasios Tsiatsis, Catherine Mulligan, Stefan Avesand, Stamatis Karnouskos, David Boyle, From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence, Academic Press.

Code: CBS.527
Course Title: Digital Forensics
Total Hours: 57

L	T	P	Cr
4	0	0	4

Course Objectives:

- Provides an in-depth study of the rapidly changing field of computer forensics.
- Introduce students to technical expertise and the knowledge required to investigate, detect and prevent digital crimes.
- Help the students understand digital forensics legislations, digital crime, forensics processes and procedures, data acquisition and validation, e-discovery tools.

Learning Outcomes:

After completion of course, students would be able to:

- Explain the relevant legislation and codes of ethics.
- Describe computer forensics, digital detective and various processes, policies and procedures.

- Examine E-discovery, guidelines and standards, E-evidence, tools and environment.
- Analyse e-mail, web forensics and network forensics.

UNIT I **15 Hours**

Digital Forensics Science: Forensics science, computer forensics, and digital forensics.
Computer Crime: Criminalistics as it relates to the investigative process, analysis of cyber-criminalistics area, holistic approach to cyber-forensics.
Legal Aspects of Digital Forensics: IT Act 2000, amendment of IT Act 2008.

UNIT II **14 Hours**

Incident- Response Methodology, Cyber Crime Scene Analysis: Discuss the various court orders etc., methods to search and seizure electronic evidence, retrieved and un-retrieved communications, Discuss the importance of understanding what court documents would be required for a criminal investigation.

UNIT III **12 Hours**

Image Capturing, Authenticating Evidence, Hidden Data Extraction, Data Storage, File Systems, Recovery of deleted files, Cracking Passwords,
Internet Crime Investigations, Web Attack Investigations.

UNIT IV **16 Hours**

Computer Forensics: Prepare a case, Begin an investigation, Understand computer forensics workstations and software, Conduct an investigation, Complete a case, Critique a case.
Network Forensics: open-source security tools for network forensic analysis, requirements for preservation of network data.
Mobile Forensics: mobile forensics techniques, mobile forensics tools

Transactional Modes:

Lecture
Case study
Demonstration
Experimentation
Discussion
Problem solving

Suggested Readings:

1. John Sammons, The Basics of Digital Forensics, Elsevier.
2. Davidoff, S. and Ham, J., Network Forensics Tracking Hackers through Cyberspace, Prentice Hall.
3. Michael G. Solomon, K Rudolph, Ed Tittel, Broom N., and Barrett D., Computer Forensics Jump Start, Willey Publishing, Inc.
4. Marcella, Albert J., Cyber forensics: A field manual for collecting, examining and preserving evidence of computer crimes, New York, Auerbach publications.

5. Davidoff, Sherri, Network forensics: Tracking hackers through cyberspace, Pearson education India private limited.

Code: CBS.525
Course Title: Secure Coding
Total Hours: 53

L	T	P	Cr
4	0	0	4

Course Objectives:
The objective of this course is to:

- Explain the most frequent programming errors leading to software vulnerabilities.
- Identify security problems in software.
- Define security threats and software vulnerabilities.

Learning Outcomes:
After completion of course, students would be able to:

- Define secure programs and disk various risk in the softwares.
- Classify various errors that lead to vulnerabilities.
- Analyze various possible security attacks.

UNIT I **11 Hours**

Software Security: Security Concepts, Security Policy, Security Flaws, Vulnerabilities, Exploitation and Mitigations. Software Security problems, Classification of Vulnerabilities.
Security Analysis: Problem Solving with static analysis: Type Checking, Style Checking, Program understanding, verifications and property checking, Bug finding and Security Review.

UNIT II **14 Hours**

Strings: Common String manipulating Errors, String Vulnerabilities and Exploits, Mitigation Strategies for strings, String handling functions, Runtime protecting strategies, Notable Vulnerabilities.
Integer Security: Integer data Type, Integer Conversions, Integer Operations, Integer Vulnerabilities, Mitigation Strategies.

UNIT III **15 Hours**

Handling Inputs: What to validate, How to validate, Preventing metadata Vulnerabilities.
Buffer Overflow: Introduction, Exploiting buffer overflow vulnerabilities, Buffer allocation strategies, Tracking buffer sizes, buffer overflow in strings, Buffer overflow in Integers Runtime protections

UNIT IV **13 Hours**

Web Applications: Input and Output Validation for the Web: Expect That the Browser Has Been Subverted, HTTP Considerations: Use POST, Not GET, Request Ordering, Error Handling, Request Provenance

Maintaining Session State: Use Strong Session Identifiers, Enforce a Session Idle Timeout and a Maximum Session Lifetime, Begin a New Session upon Authentication.

Transactional Modes:
Lecture
Case study
Demonstration
Experimentation
Discussion
Problem solving

Suggested Readings:

1. Seacord, R. C., Secure Coding in C and C++, Addison Wisley.
2. Chess, B., and West, J., Secure Programming with static Analysis, Addison Wisley.
3. Seacord, R. C., The CERT C Secure Coding Standard, Pearson Education.
4. Howard, M., LeBlanc, D., Writing Secure Code, Pearson Education.

L	T	P	Cr
4	0	0	4

Code: CST.529
Course Title: Blockchain Technology
Total Hours: 63

Course Objectives:
The objective of this course is to introduce students to:
- Define the concept of Blockchain, Crypto Primitives, Bitcoin Basics.
- Explain distributed Consensus, and Consensus in Bitcoin
- Discuss Permissioned Blockchain, and Hyperledger Fabric.

Learning Outcomes:
After completion of course, students would be able to:
- Describe the basic concept of Blockchain, Crypto Primitives, Bitcoin Basics
- Identify the area in which they can apply permission or permission less blockchain.
- Apply Block chaining concept in various applications.

UNIT I **15 Hours**
Introduction to Blockchain: What is Blockchain, Public Ledgers, Blockchain as Public Ledgers, Bitcoin, Blockchain 2.0, Smart Contracts, Block in a Blockchain, Transactions, Distributed Consensus, The Chain and the Longest Chain, Cryptocurrency to Blockchain 2.0, Permissioned Model of Blockchain

UNIT II **15 Hours**

Basic Crypto Primitives: Cryptographic Hash Function, Properties of a hash function, Hash pointer and Merkle tree, Digital Signature, Public Key Cryptography, A basic cryptocurrency.

Bitcoin Basics: Creation of coins, Payments and double spending, FORTH – the precursor for Bitcoin scripting, Bitcoin Scripts, Bitcoin P2P Network, Transaction in Bitcoin Network, Block Mining, Block propagation and block relay.

UNIT III **16 Hours**

Distributed Consensus: Why Consensus, Distributed consensus in open environments, Consensus in a Bitcoin network.

Consensus in Bitcoin: Bitcoin Consensus, Proof of Work (PoW) – basic introduction, Hashcash PoW, Bitcoin PoW, Attacks on PoW and the monopoly problem, Proof of Stake, Proof of Burn and Proof of Elapsed Time. The life of a Bitcoin Miner, Mining Difficulty, Mining Pool.

Permissioned Blockchain: Permissioned model and use cases, Design issues for Permissioned blockchains, Execute contracts, State machine replication, Consensus models for permissioned blockchain, Distributed consensus in closed environment, Paxos, RAFT Consensus, Byzantine general problem.

UNIT IV **17 Hours**

Blockchain Components and Concepts: Actors in a Blockchain, Components in Blockchain design, Ledger in Blockchain.

Hyperledger Fabric – Transaction Flow: Fabric Architecture, Transaction flow in Fabric.

Hyperledger Fabric Details: Ordering Services, Channels in Fabric, Fabric Peer and Certificate Authority.

Fabric – Membership and Identity Management: Organization and Consortium Network, Membership Service Provide, Transaction Signing.

Transactional Modes:

Lecture
Case study
Demonstration
Experimentation
Discussion
Problem solving

Suggested Readings:

1. Nitin Gaur, Luc Desrosiers, Venkatraman Ramakrishna, Petr Novotny, Salman Baset, Anthony O'Dowd.Hands-On Blockchain with Hyperledger: Building decentralized applications with Hyperledger Fabric and Composer. Packt Publishing Ltd.
2. Bellaj Badr, Richard Horrocks, Xun (Brian) Wu. Blockchain By Example: A developer's guide to creating decentralized applications using Bitcoin, Ethereum, and Hyperledger. Packt Publishing Ltd, 2018.

3. Vikram Dhillon, David Metcalf, Max Hooper. Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You. Apress.
4. Mayukh Mukhopadhyay Ethereum Smart Contract Development: Build blockchain-based decentralized applications using solidity. Packt Publishing Ltd.

Code: CBS.526
Course Title: Security Assessment & Risk Analysis
Total Hours: 57

L	T	P	Cr
4	0	0	4

Course Objectives:
The objective of this course is to:

- To introduce students to the concepts of risk management.
- Define and differentiate various Contingency Planning components.
- Integrate the IRP, DRP, and BCP plans into a coherent strategy to support sustained organizational operations.
- Define and be able to discuss incident response options, and design an Incident Response Plan for sustained organizational operations.

Learning Outcomes:
After completion of course, students would be able to:

- State contingency strategies including data backup and recovery and alternate site selection for business resumption planning
- Describe the escalation process from incident to disaster in case of security disaster.
- Design a Disaster Recovery Plan for sustained organizational operations.
- Design a Business Continuity Plan for sustained organizational operations.

UNIT I **16 Hours**

SECURITY BASICS: Information Security (INFOSEC) Overview: critical information characteristics – availability information states – processing security Countermeasures- education, training and awareness, critical information characteristics – confidentiality critical information characteristics – integrity, information states – storage, information states – transmission, security countermeasures-policy, procedures and practices, threats, vulnerabilities.

UNIT II **15 Hours**

Threats to and Vulnerabilities of Systems: definition of terms (e.g., threats, vulnerabilities, risk), major categories of threats (e.g., fraud, Hostile Intelligence Service (HOIS), malicious logic, hackers, environmental and technological hazards, disgruntled employees, careless employees, HUMINT, and monitoring), threat impact areas, Countermeasures: assessments (e.g., surveys, inspections), Concepts of Risk Management: consequences (e.g., corrective action, risk assessment), cost/benefit analysis of controls,

implementation of cost-effective controls, monitoring the efficiency and effectiveness of controls (e.g., unauthorized or inadvertent disclosure of information), threat and vulnerability assessment.

UNIT III **17 Hours**

Security Planning: directives and procedures for policy mechanism, Risk Management: acceptance of risk (accreditation), corrective actions information identification, risk analysis and/or vulnerability assessment components, risk analysis results evaluation, roles and responsibilities of all the players in the risk analysis process, Contingency Planning/Disaster Recovery: agency response procedures and continuity of operations, contingency plan components, determination of backup requirements, development of plans for recovery actions after a disruptive event, development of procedures for off-site processing, emergency destruction procedures, guidelines for determining critical and essential workload, team member responsibilities in responding to an emergency situation.

UNIT IV **18 Hours**

Policies and Procedures

Physical Security Measures: alarms, building construction, cabling, communications centre, environmental controls (humidity and air conditioning), filtered power, physical access control systems (key cards, locks and alarms) Personnel Security Practices and Procedures: access authorization/verification (need-to-know), contractors, employee clearances, position sensitivity, security training and awareness, systems maintenance personnel, Administrative Security Procedural Controls: attribution, copyright protection and licensing, Auditing and Monitoring: conducting security reviews, effectiveness of security programs, investigation of security breaches, privacy review of accountability controls, review of audit trails and logs.

Operations Security (OPSEC): OPSEC surveys/OPSEC planning INFOSEC: computer security – audit, cryptography-encryption (e.g., point-to-point, network, link), cryptography-key management (to include electronic key), Cryptography-strength (e.g., complexity, secrecy, characteristics of the key) Case study of threat and vulnerability assessment.

Transactional Modes:

Lecture
Case study
Demonstration
Experimentation
Discussion
Problem solving

Suggested Readings:

1. Whitman & Mattord, Principles of Incident Response and Disaster Recovery, Course Technology, ISBN: 141883663X
2. (Web Link) http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf

Code: CBS.528
Course Title: Python Programming for Security Professionals
Total Hours: 63

L	T	P	Cr
4	0	0	4

Course Objectives:
The objective of this course is to:

- Introduces the concepts of Python Programming.
- Gives the students the opportunity to learn Python Modules.
- Practically develop Python code to perform various activities.

Learning Outcomes:
After completion of course, students would be able to:

- Use basics python programming constructs and various Python modules required for accessing operating system and Network.
- Write scripts in Python language for Network related activities.
- Prepare python scripts to perform activities related to forensics.

UNIT I **16 Hours**

Python Introduction, Installing and setting Python environment in Windows and Linux, basics of Python interpreter, Execution of python program, Editor for Python code, syntax, variable, types. Flow control: if, ifelse, for, while, range() function, continue, pass, break. Strings: Sequence operations, String Methods, Pattern Matching.

UNIT II **16 Hours**

Lists: Basic Operations, Iteration, Indexing, Slicing and Matrixes; Dictionaries: Basic dictionary operations; Tuples: Basic Tuple operations; Functions: Definition, Call, Arguments, Scope rules and Name resolution; Modules: Module Coding Basics, Importing Programs as Modules, Executing Modules as Scripts, Compiled Python files(.pyc), Standard Modules: OS and SYS, The dir() Function, Packages.

UNIT III **14 Hours**

Input output and file handling, Object Oriented Programming features in Python: Classes, Objects, Inheritance, Operator Overloading, Errors and Exceptions: try, except and else statements, Exception Objects, Regular expressions, Multithreading, Modules to handle multidimensional data: Numpy, Panadas, Files.

UNIT IV **17 Hours**

Networking: Socket module, Port Scanning, Packet Sniffing, Traffic Analysis, TCP Packet Injection, Log analysis.
HTTP Communications with Python built in Libraries, Web communications with the Requests module, Forensic Investigations with Python: geo-locating, recovering deleted items, examining metadata and windows registry.

Transactional Modes:
Lecture
Case study

Demonstration
Experimentation
Discussion
Problem solving

Suggested Readings:

1. Lutz Mark, Learning Python, Latest Edition., O'REILLY Media, Inc.
2. TJ. O'Connor, Violent Python A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers, Elsevier.
3. Seitz Justin , Gray Hat Python: Python Programming with Hackers and Reverse Engineers, Latest Edition, No Starch Press, Inc.
4. Seitz Justin , Black Hat Python: Python Programming for Hackers and Pentesters, Latest Edition, No Starch Press, Inc
5. Berry Paul, Head First Python. Latest Edition, O'REILLY Media, Inc.

Code: CST.527
Course Title: Soft Computing Lab

L	T	P	Cr
0	0	4	2

Course Objectives:
The objective of this course is to:

- The primary objective of soft-computing lab is to provide a practical introduction to various techniques in soft computing and their applications.
- Enable students to apply the soft-computing techniques to various real life Practical problems.

Course outcome:
After Completion of the lab course the students will be able to:

- Implement simple applications using the fuzzy logic.
- Understand the various types of neural networks and write programmes to implement the same.
- Learn optimization based on GA and implement some of its application.

Students will implement the lab practical as per the syllabus of the subject.

List of Practical based on:
Lab Evaluation:

The evaluation of lab criteria will be based on following parameters:

Component	**Marks**
Continuous Evaluation	30
End Term (Implementation and Viva-Voce)	20
Total	**50**

Code: CBS.529
Course Title: Python Programming for Security Professionals Lab

L	T	P	Cr
0	0	4	2

Course Objective:

- By the end of the course, students will have gained a fundamental understanding of programming in Python by creating a variety of scripts to perform cyber security related activities.
- The objective of this course is to enable the students to explore the large standard library of Python 3, which supports many common cyber security tasks.

Learning Outcomes:

Upon successfully completing this course, students will be able to "do something useful with Python".

- Understand Python Syntax.
- Design a program to solve the problem.
- Create scripts to perform various cyber security activities.
- Write basic unit tests.

Students will implement the lab practical as per the syllabus of the subject.

List of Practical based on:
Lab Evaluation:

The evaluation of lab criteria will be based on following parameters:

Component	**Marks**
Continuous Evaluation	30
End Term (Implementation and Viva-Voce)	20
Total	**50**

SEMESTER -III

Code: CBS.551
Course Title: Biometric Security
Total Hours: 56

L	T	P	Cr
4	0	0	4

Course Objectives:

- Introduce Bio-metric and traditional authentication methods.
- Describe the background theory and types of features used in biometric techniques and algorithms related to various biometrics.
- Evaluate the performance of various biometric systems.

Learning Outcomes:

After completion of course, students would be able to:

- Describe the various modules constituting a bio-metric system. Compare and contrast the different bio-metric traits and appreciate their relative significance.
- Classify the different feature sets used to represent some of the popular bio-metric traits.
- Evaluate and design security systems incorporating bio-metrics.

UNIT I **15 Hours**

Introduction and Definitions of bio-metrics, Traditional authenticated methods and technologies. Introduction to Image Processing, Image Enhancement Techniques**:** Spatial Domain Methods: Smoothing, sharpening filters, Laplacian filters, Frequency domain filters, Smoothing and sharpening filters.

UNIT II **15 Hours**

Image Restoration & Reconstruction: Model of Image Degradation/restoration process, Noise models, spatial filtering, inverse filtering, Minimum mean square Error filtering.

Introduction to image segmentation: Image edge detection: Introduction to edge detection, types of edge detectors. Introduction to image feature extraction.

UNIT III **21 Hours**

Bio-metric technologies: Fingerprint, Face, Iris, Hand Geometry, Gait recognition, Ear, Voice, Palm print, On-Line Signature Verification, 3D Face, Recognition, Dental Identification and DNA.

UNIT IV **15 Hours**

The Law and the use of multi bio-metrics systems. Statistical measurement of Bio-metric.

Bio-metrics in Government Sector and Commercial Sector. Case Studies of bio-metric system, Bio-metric Transaction. Bio-metric System Vulnerabilities.

Recent trends in Bio-metric technologies and applications in various domains. Case study of 3D face recognition and DNA matching.

Transactional Modes:

Lecture
Case study
Demonstration
Experimentation
Discussion
Problem solving

Suggested Readings:

1. Paul Reid, Biometrics for network security, Hand book of Pearson.
2. D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer Verlag.

3. K. Jain, R. Bolle, S. Pankanti (Eds.), BIOMETRICS: Personal Identification in Networked Society, Kluwer Academic Publishers.
4. J. Wayman, A.K. Jain, D. Maltoni, and D. Maio (Eds.), Biometric Systems: Technology.
5. Design and Performance Evaluation, Springer.
6. Anil Jain, Arun A. Ross, Karthik Nanda kumar, Introduction to biometric, Springer.
7. Biometric Systems: Technology, Design and Performance Evaluation, J. Wayman, A.K. Jain, D. Maltoni, and D. Maio.
8. Gonzalez, R.C. and Woods, R.E., Digital Image Processing India: Person Education.

Code: CST.552
Course Title: Data Warehousing and Data Mining
Total Hours: 62

L	T	P	Cr
4	0	0	4

Course Objectives:
The objective of this course is to
- Introduce data warehousing and mining techniques.
- To make the students aware of broad data mining areas and their application in web mining, pattern matching and cluster analysis is included.

Learning Outcomes:
After completion of course, students would be able to:
- Define sequential pattern algorithms.
- Describe the technique to extract patterns from time series data and it application in real world.
- Use graph mining algorithms for Web mining.
- Design the computing framework for Big Data.

UNIT I **14 Hours**
Introduction to Data Warehousing: Data warehousing Architecture, OLAP Server, Data warehouse Implementation.
Data Mining: Mining frequent patterns, association and correlations; Sequential Pattern Mining concepts, primitives, scalable methods;

UNIT II **15 Hours**
Classification and prediction: Cluster Analysis – Types of Data in Cluster Analysis, Partitioning methods, Hierarchical Methods; Transactional Patterns and other temporal based frequent patterns.

UNIT III **16 Hours**
Mining Time series Data, Periodicity Analysis for time related sequence data, Trend analysis, Similarity search in Time-series analysis;
Mining Data Streams, Methodologies for stream data processing and stream data systems, Frequent pattern mining in stream data, Sequential Pattern Mining in Data Streams, Classification of dynamic data streams.

UNIT IV **17 Hours**

Web Mining, Mining the web page layout structure, mining web link structure, mining multimedia data on the web, Automatic classification of web documents and web usage mining; Distributed Data Mining.
Recent trends in Distributed Warehousing and Data Mining, Class Imbalance Problem; Graph Mining; Social Network Analysis.

Transactional Modes:

Lecture
Case study
Demonstration
Experimentation
Discussion
Problem solving

Suggested Readings:

1. Jiawei Han and M Kamber, Data Mining Concepts and Techniques, Second Edition, Elsevier Publication.
2. Vipin Kumar, Michael Steinbach, Introduction to Data Mining - Pang-Ning Tan, Addison Wesley.
3. G Dong and J Pei, Sequence Data Mining, Springer.

Code: CST.553
Course Title: Introduction to Intelligent Systems
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:

The objective of this course is to:

- Introduce the field of Artificial Intelligence (AI) to solve real world problems for which solutions are difficult to express using the traditional algorithmic approach.
- Help students understand essential theory behind methodologies for developing systems that demonstrate intelligent behaviour including dealing with uncertainty, learning from experience and following problem solving strategies found in nature.

Learning Outcomes:

After completion of course, students would be able to:

- Explain the fundamental principles of intelligent systems.
- Analyse and compare the relative merits of a variety of AI problem solving techniques.

UNIT I **15 Hours**

Search Methods Basic concepts of graph and tree search. Three simple search methods: breadth-first search, depth-first search, iterative deepening search. Heuristic search methods: best-first search, admissible

evaluation functions, hill climbing search. Optimization and search such as stochastic annealing and genetic algorithm.

UNIT II **15 Hours**

Knowledge representation and logical inference Issues in knowledge representation. Structured representation, such as frames, and scripts, semantic networks and conceptual graphs. Formal logic and logical inference. Knowledge-based systems structures, its basic components. Ideas of Blackboard architectures.

UNIT III **15 Hours**

Reasoning under uncertainty and Learning Techniques on uncertainty reasoning such as Bayesian reasoning, Certainty factors and Dempster-Shafer Theory of Evidential reasoning, A study of different learning and evolutionary algorithms, such as statistical learning and induction learning.

UNIT IV **15 Hours**

Biological foundations to intelligent systems I: Artificial neural networks, Back propagation
Networks, Radial basis function networks, and recurrent networks.
Biological foundations to intelligent systems II: Fuzzy logic, knowledge Representation and inference mechanism, genetic algorithm, and fuzzy neural networks.
Recent trends in Fuzzy logic, Knowledge Representation

Transactional Modes:

Lecture
Case study
Demonstration
Experimentation
Discussion
Problem solving

Suggested Readings:

1. Luger G.F. and Stubblefield W.A., Artificial Intelligence: Structures and strategies for Complex Problem Solving, Addison Wesley.
2. Russell S. and Norvig P. , Artificial Intelligence: A Modern Approach, Prentice-Hall.

Code: CST.554
Course Title: Mobile Applications & Service
Total Hours: 62

L	T	P	Cr
4	0	0	4

Course Objectives:

The objective of the course is to:

- Introduce students to three main mobile platforms and their ecosystems, namely Android, iOS, and PhoneGap/Web OS.

- Help the students explores emerging technologies and tools used to design and implement feature-rich mobile applications for smartphones and tablets

Learning Outcomes:

After completion of course, students would be able to:

- Identify the target platform and users and be able to define and sketch a mobile application.
- Discuss the fundamentals, frameworks, and development lifecycle of mobile application platforms including iOS, Android, and PhoneGap.
- Design and develop a mobile application prototype in one of the platform (challenge project).

UNIT I **14 Hours**

Introduction: Introduction to Mobile Computing, Introduction to Android Development Environment, Factors in Developing Mobile Applications, Mobile Software Engineering, Frameworks and Tools, Generic UI Development Android User.

UNIT II **15 Hours**

More on Uis: VUIs and Mobile Apps, Text-to-Speech Techniques, Designing the Right UI, Multichannel and Multimodal Uis, . Storing and Retrieving Data, Synchronization and Replication of Mobile Data, Getting the Model Right, Android Storing and Retrieving Data, Working with a Content Provider

UNIT III **16 Hours**

Communications via Network and the Web: State Machine, Correct Communications Model, Android Networking and Web, Telephony Deciding Scope of an App, Wireless Connectivity and Mobile Apps, Android Telephony Notifications and Alarms-Performance, Performance and Memory Management, Android Notifications and Alarms, Graphics, Performance and Multithreading, Graphics and UI Performance, Android Graphics.

UNIT IV **17 Hours**

Putting It All Together: Packaging and Deploying, Performance Best Practices, Android Field Service App, Location Mobility and Location Based Services Android Multimedia: Mobile Agents and Peer-to-Peer Architecture, Android Multimedia Platforms and Additional Issues: Development Process, Architecture, Design, Technology Selection, Mobile App Development Hurdles, Testing, Security and Hacking, Active Transactions, More on Security, Hacking Android.

Recent trends in Communication protocols for IOT nodes, mobile computing techniques in IOT, agents based communications in IOT.

Transactional Modes:

Lecture
Case study
Demonstration

Experimentation
Discussion
Problem solving

Suggested Readings:

1. Wei-Meng Lee, Beginning Android TM 4 Application Development, John Wiley & Sons.

Code: CBS.552
Course Title: Cyber threat Intelligence
Total Hours: 62

L	T	P	Cr
4	0	0	4

Course Objectives:

The objective of this course is to:

- Introduce students to the cyber threats and Cyber Threat Intelligence Requirements
- Help students to classify cyber threat information
- Examine the potential for incidents and, provide more thoughtful responses.

Learning Outcomes:

After completion of course, students would be able to:

- Describe different Cyber Threat.
- Explain technique to Develop Cyber Threat Intelligence Requirements.
- Analyze and Disseminating Cyber Threat Intelligence

UNIT I **15 Hours**

Defining Cyber Threat Intelligence: The Need for Cyber Threat Intelligence: The menace of targeted attacks, The monitor-and-respond strategy, Why the strategy is failing, Cyber Threat Intelligence Defined, Key Characteristics: Adversary based, Risk focused, Process oriented, Tailored for diverse consumers, The Benefits of Cyber Threat Intelligence

UNIT II **14 Hours**

Developing Cyber Threat Intelligence Requirements: Assets That Must Be Prioritized: Personal information, Intellectual property, Confidential business information, Credentials and IT systems information, Operational systems. Adversaries: Cybercriminals, Competitors and cyber espionage agents, Hacktivists. Intelligence Consumers: Tactical users, Operational users, Strategic users

UNIT III **17 Hours**

Collecting Cyber Threat Information: Level 1: Threat Indicators, File hashes and reputation data, Technical sources: honeypots and scanners, Industry sources: malware and reputation feeds. Level 2: Threat Data Feeds, Cyber threat statistics, reports, and surveys, Malware analysis. Level 3: Strategic

Cyber Threat Intelligence, Monitoring the underground, Motivation and intentions, Tactics, techniques, and procedures.
Analyzing and Disseminating Cyber Threat Intelligence: Information versus Intelligence, Validation and Prioritization: Risk scores, Tags for context, Human assessment. Interpretation and Analysis: Reports, Analyst skills, Intelligence platform, Customization. Dissemination: Automated feeds and APIs, Searchable knowledge base, Tailored reports.

UNIT IV **16 Hours**

Selecting the Right Cyber Threat Intelligence Partner: Types of Partners: Providers of threat indicators, Providers of threat data feeds, Providers of comprehensive cyber threat intelligence. Important Selection Criteria: Global and cultural reach, Historical data and knowledge, Range of intelligence deliverables, APIs and integrations, Intelligence platform, knowledge base, and portal, Client services, Access to experts. Intelligence-driven Security.

Transactional Modes:

Lecture
Case study
Demonstration
Experimentation
Discussion
Problem solving

Suggested Readings:

1. Jon Friedman. Mark Bouchard, CISSP. Foreword by John P. Watters, Cyber Threat Intelligence, Definitive Guide TM.
2. Scott J. Roberts, Rebekah Brown, Intelligence- Driven Incident Response: Outwitting the Adversary, O'Reilly Media.
3. Henry Dalziel, How to Define and Build an Effective Cyber Threat Intelligence Capability Elsevier Science & Technology.
4. John Robertson, Ahmad Diab, Ericsson Marin, Eric Nunes, Vivin Paliath, Jana Shakarian, Paulo Shakarian, DarkWeb Cyber Threat Intelligence Mining Cambridge University Press.
5. Bob Gourley, The Cyber Threat, Createspace Independent Pub.

Code: CST.556
Course Title: Cost Management of Engineering Projects
Total Hours: 55

L	T	P	Cr
4	0	0	4

UNIT I **11 Hours**

Introduction and Overview of the Strategic Cost Management Process
Cost concepts in decision-making; Relevant cost, Differential cost, Incremental cost and Opportunity cost. Objectives of a Costing System; Inventory valuation; Creation of a Database for operational control; Provision of data for Decision-Making.

UNIT II **14 Hours**

Project: meaning, Different types, why to manage, cost overruns centers, various stages of project execution: conception to commissioning. Project execution as conglomeration of technical and nontechnical activities. Detailed Engineering activities. Pre project execution main clearances and documents Project team: Role of each member. Importance Project site: Data required with significance.

Project contracts. Types and contents. Project execution Project cost control. Bar charts and Network diagram. Project commissioning: mechanical and process.

UNIT III **14 Hours**

Cost Behavior and Profit Planning Marginal Costing; Distinction between Marginal Costing and Absorption Costing; Break-even Analysis, Cost-Volume-Profit Analysis. Various decision-making problems. Standard Costing and Variance Analysis. Pricing strategies: Pareto Analysis. Target costing, Life Cycle Costing. Costing of service sector. Just-in-time approach, Material Requirement Planning, Enterprise Resource Planning, Total Quality Management and Theory of constraints.

UNIT IV **15 Hours**

Activity-Based Cost Management, Bench Marking; Balanced Score Card and Value-Chain Analysis. Budgetary Control; Flexible Budgets; Performance budgets; Zero-based budgets. Measurement of Divisional profitability pricing decisions including transfer pricing.

Quantitative techniques for cost management, Linear Programming, PERT/CPM, Transportation problems, Assignment problems, Simulation, Learning Curve Theory.

Transactional Modes:

Lecture
Case study
Demonstration
Experimentation
Discussion
Problem solving

Suggested Readings:

1. Charles T. Horngren, Srikant M. Datar, Cost Accounting a Managerial Emphasis, Pearson.
2. Ahmed Riahi- Belkaoui., Advanced Management Accounting, Greenwood Publication Group.
3. Robert S Kaplan Anthony A. Alkinson, Management Accounting, Prentice Hall.
4. Ashish K. Bhattacharya, Principles & Practices of Cost Accounting A. H. Wheeler publisher.
5. N.D. Vohra, Quantitative Techniques in Management, Tata McGraw Hill Book Co. Ltd.

Code: CBS.553
Course Title: Cyber Law
Total Hours: 50

L	T	P	Cr
4	0	0	4

Course Objectives:
The objective of this course is to provide knowledge about the basic information on IT Act and Cyber law as well as the legislative and judicial development in the area.

Learning Outcomes:
After completion of course, students would be able to:

- Analyze fundamentals of Cyber Law.
- Discuss IT Act & its Amendments.
- Relate Cyber laws with security incidents.

UNIT I **9 Hours**
Concept of Cyberspace, Issues of Jurisdiction in Cyberspace: Jurisdiction Principles under International law, Jurisdiction in different states, Position in India. Conflict of Laws in Cyberspace, International Efforts for harmonization Privacy in Cyberspace.

UNIT II **13 Hours**
Electronic Commerce, Cyber Contract, Intellectual Property Rights and Cyber Laws. UNCITRAL Model Law, Digital Signature and Digital Signature Certificates, E-Governance and Records.

UNIT III **14 Hours**
Define Crime, *Mens Rea*, Crime in Context of Internet, Types of Cyber Crime, Computing Damage in Internet Crime, Offences under IPC (Indian Panel Code, 1860), Offences & Penalties under IT Act 2000, IT Act Amendments, Investigation & adjudication issues, Digital Evidence.

UNIT IV **14 Hours**
Obscenity and Pornography, Internet and potential of Obscenity, International and National Instruments on Obscenity & Pornography, Child Pornography,
Important Case Studies.

Transactional Modes:
Lecture
Case study
Demonstration
Experimentation
Discussion
Problem solving

Suggested Readings:

1. Dr. Farooq Ahmad, Cyber Law in India, Allahbad Law Agency-Faridabad.
2. J.P. Sharma, Sunaina Kanojia, Cyber Laws.
3. Harish Chander , Cyber Laws and IT Protection
4. Justice Yatindra Singh, Cyber Laws.
5. Prof. R.K. Chaubey, An Introduction to cyber-crime and cyber law.
6. Garima Tiwari, Understanding Laws.
7. Karnika Seth, Justice Altamas Kabir, Computers Internet and New Technology Laws.

Code: CST.557
Course Title: Software Metrics
Total Hours: 58

L	T	P	Cr
4	0	0	4

Course Objectives:

The objective of this course is

- Understand the underlying concepts, principles and practices in Software Measurements.
- Designing of Metrics model for software quality prediction and reliability.

Learning Outcomes:

After completion of course, students would be able to:

- Learn role software Metrics in Industry size software
- Empirically investigate software for a quality measurement.
- Identify software reliability and problem solving by designing and selecting software reliability models.

UNIT I **14 Hours**

Overview of Software Metrics: Measurement in Software Engineering, Scope of Software Metrics, Measurement and Models Meaningfulness in measurement, Measurement quality, Measurement process, Scale, Measurement validation, Object-oriented measurements.

Goal based framework for software measurement: Software measure classification, Goal-Question-Metrics(GQM) and Goal-Question-Indicator-Metrics (GQIM), Applications of GQM and GQIM.

UNIT II **15 Hours**

Empirical Investigation: Software engineering investigation, Investigation principles, Investigation techniques, Planning Formal experiments, Case Studies for Empirical investigations.

Object–oriented metrics: Object-Oriented measurement concepts, Basic metrics for OO systems, OO analysis and design metrics, Metrics for productivity measurement, Metrics for OO software quality.

UNIT III **16 Hours**

Measuring Internal Product attributes: Software Size, Length, reuse, Functionality, Complexity, Software structural measurement, Control flow structure, Cyclomatic Complexity, Data flow and data structure attributes Architectural measurement.

Measuring External Product attributes: Software Quality Measurements, Aspectes of Quality Measurements, Maintainability Measurements, Usability and Security Measurements.

UNIT IV **13 Hours**

Measuring software Reliability: Concepts and definitions, Software reliability models and metrics, Fundamentals of software reliability engineering (SRE), Reliability management model.

Transactional Modes:

Lecture
Case study
Demonstration
Experimentation
Discussion
Problem solving

Suggested Readings:

1. Norman E. Fenton, S. L. P fleeger, Software Metrics: A Rigorous and Practical Approach, published by International Thomson Computer Press.
2. Stephen H. Kan, Metrics and Models in Software Quality Engineering, Addison-Wesley Professional.
3. Basu Anirban, Software Quality Assurance, Testing and Metrics, Prentice Hall India Learning Private Limited.
4. Robert B. Grady, Practical Software Metrics for Project Management and Process Improvement, Prentice Hall.
5. Maxwell Katrina D., Applied Statistics for Software Managers, Prentice Hall PTR.

Code: CBS.600
Course Title: Dissertation/ Industrial Project

L	T	P	Cr
0	0	10	5

Course Objectives:

The objective of this course is

- The student shall have to write his/ her synopsis including an extensive review of literature with simultaneous identification of scientifically sound (and achievable) objectives backed by a comprehensive and detailed methodology. The students shall also present their synopsis to the synopsis approval committee.
- The second objective of Dissertation would be to ensure that the student learns the nuances of the scientific research. Herein the student shall have to carry out the activities/experiments to be

completed during Dissertation (as mentioned in the synopsis).

Course Outcome

- The students would present their work to the Evaluation Committee (constituted as per the university rules). The evaluation criteria shall be as detailed below:

Evaluation criteria for Synopsis:

Evaluation Parameter	**Marks**	**Evaluated by**
Review of literature	50	**Internal Evaluation by Dean of School, HOD/ HOD nominee, Two faculty member nominated by Dean/HOD, Supervisor.**
Identification of gaps in knowledge and Problem Statement, Objective formulation & Methodology	50	
Total	**100**	

Student will be given final marks based the average marks by the Evaluation Committee

Timeline Works for Synopsis and Mid-Term:

Month	**JULY**	**AUG**	**SEP**	**OCT**	**NOV**	**DEC**
Synopsis	Bi- Weekly report submitted to Supervisor	Submission of Synopsis and Presentation				
Mid-Term			Bi-Weekly report submitted to Supervisor	Report submission in 3rd week Final Presentation in 4th week	Final Submission of Mid Term Report	

Grading of Marks:

Grades	A	B	C	D	E
Marks	85-100	84-75	74-65	64-40	0-40

Grading Evaluation:

Abbreviations of Grades	**Grades**
Excellent	A
Very Good	B
Good	C
Average	D
Below Average/ Un-Satisfactory	E

Evaluation criteria for Mid-Term:

Evaluation Parameter	Max. Marks	Evaluated By
Mid Term Review and Presentation	50	**Internal/External Evaluation by Dean of School, HOD/ HOD nominee, Two faculty member nominated by Dean/ HOD, Supervisor.**
Continuous evaluation	50	
Total	**100**	

Code: CBS.559
Course Title: Capstone Lab

L	T	P	Cr
0	0	2	2

In this, the student has to select an area and specify the base paper in that area to implement the same and show the results.
Evaluation criteria will be based on objectives stated and achieved

Course Objective:

- The objective of this lab is to help a team of students develop and execute an innovative project idea under the direction of the Capstone course Incharge.

Course Outcome:
After the completion of the course the students will be able to

- Complete the four phases of project development: requirements analysis, design, implementation, and documentation.

Timeline Work of Seminar:

Month	AUG	SEP	NOV
Work to be Done	Submit area and Objectives to be achieved	Weekly report to faculty Incharge.	3rd week submit report 4th week Presentation

Evaluation Criteria:

Evaluation Parameter	Marks	Evaluated By
Area & Objectives	5	**Evaluation Committee**
Reports and Implementation	10	
Presentation and Viva-voce	10	
Total	**25**	

Student will be given final marks based the average marks by the Evaluation Committee

SEMESTER –IV

Code: CBS.600
Course Title: Dissertation

L	T	P	Cr
0	0	16	8

Course Objectives:
In Dissertation the student shall have to carry out the activities/ experiments to be completed during Dissertation (as mentioned in the synopsis).

Course Outcomes:
The students would present their work to the evaluation Committee (constituted as per the university rules).
One research paper (either communicated to a Journal or accepted/ presented/published in a conference proceedings) out of the dissertation research work is compulsory. The Evaluation criteria shall be as detailed below:

Evaluation Parameter	Maximum Marks	Evaluated By
Parameters by External Expert (As per University Criteria)	50	**Internal/External Evaluation by Dean of School, DAA Nominee, HOD/ HOD nominee, Supervisor.**
Presentation and defence of research work	50	
Total	100	

Student will be given final marks based the average marks by the Evaluation Committee

Timeline Work of Dissertation:

Month	JAN	FEB	MAR	APR	MAY	JUN
Dissertation	Bi-Weekly report submitted to Supervisor	Bi-Weekly report submitted to Supervisor	Report submission in 1st week	Pre-Submission Presentation in 3st week Report submission in 4th week	Final Submission of Dissertation/ Industrial Project and External Evaluation	

Grading of Marks:

Grades	A	B	C	D	E
Marks	85-100	84-75	74-65	64-40	0-40

Grading Evaluation:

Abbreviations of Grades	Grades
Excellent	A
Very Good	B
Good	C
Average	D
Below Average/ Un-Satisfactory	E