Master of Technology in Computer Cyber Security

Course Structure and Syllabus

1st to 4th Semester

Academic Session 2018-19

Department of Computer Science & Technology

Central University of Punjab

Bathinda

Master's Programme Course Structure

School: Engineering & Technology							
Department: Computer Science & Technology							
Programme: M-Tech. Computer Science & Technology (Cyber Security)							
Batch: 2018-19							
Semester- I							
S. No.	**Course Code**	**Course Title**	**Course Type**	**Credit Hours**			
				L	**T**	**P**	**Total credit**
1.	CST-507	Mathematical Foundation of Computer Science	Core-I	4	0	0	4
2.	CST-506	Advanced Data Structure and Algorithms	Core-II	4	0	0	4
3.	CBS-506	Ethical Hacking	Elective-I	4	0	0	4
	CBS-507	Intrusion Detection					
4.	CBS-508	Data Encryption & Network Security	Elective-II	4	0	0	4
	CBS-509	Information Theory					
	CST-508	Machine Learning					
5.	CST. 514	Research Methodology	Foundation	4	0	0	4
6.	XXX.YYY	Opt any one course from the courses offered by the University	IDC	2	0	0	2
7.	XXX.YYY	Opt any one course from the courses offered by the University	Value Added	2	0	0	2
8.	CST-515	Advanced Data Structure - Lab	Laboratory-I	0	0	4	2
9.	CBS-510	Ethical Hacking- Lab	Laboratory-II	0	0	4	2
	CBS-511	Intrusion Detection - Lab					
			Total	24	0	8	**28**

Semester-II

S. No.	**Course Code**	**Course Title**	**Course Type**	**Credit Hours**			
				L	**T**	**P**	**Total credit**
1.	CST-521	Advance Algorithm	Core-III	4	0	0	4
2.	CST-522	Soft Computing	Core-IV	4	0	0	4
3.	CBS.521	Malware Analysis & Reverse Engineering		4	0	0	4
	CBS-522	Steganography					

	CBS-523	Secure Software Design & Enterprise Computing	Elective-III				
	CBS-524	Big Data Analysis and Visualization					
	CST-524	IOT (Internet of Things)					
4.	CBS-525	Secure Coding	Elective-IV	4	0	0	4
	CBS-526	Security Assessment & Risk Analysis					
	CBS-527	Digital Forencies					
5.	CBS-528	Python Programming for Security Professionals	Skill Development	4	0	0	4
6.	XXX.YYY	Inter Disciplinary Course (IDC)	IDC	2	0	0	2
7.	CST.527	Soft Computing-Lab	Laboratory-I	0	**0**	**4**	2
8.	CBS.529	Python Programming for Security Professionals - Lab	Laboratory-II	0	**0**	**4**	2
			Total	22	0	8	**26**

Semester-III

S. No.	Course Code	Course Title	Course Type	Credit Hours			
				L	T	P	Total credit
1.	CBS.551	Biometric Security	Elective	4	0	0	4
	CST-552	Data Warehousing and Data Mining					
	CST.553	Introduction to Intelligent System					
	CST.554	Mobile Applications & Services					
2.	CBS-552	Cyber Threat Intelligence	Open Elective	4	0	0	4
	CST.555	Operations Research					
	CST.556	Cost Management of Engineering Projects					
	CBS-553	Cyber Law					
	CST.557	Software Metrics					
3.	CBS.543	Seminar with Minor Project		0	0	2	2
4.	CBS.600	Dissertation/ Industrial Project		0	0	10	10
			Total	8	0	12	**20**

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

Semester : IV							
S. No.	**Course Code**	**Course Title**	**Course Type**	**Credit Hours**			
				L	**T**	**P**	**Total credit**
1.	CBS.600	Dissertation				16	16
			Total			16	**16**

A: Continuous Assessment: Based on Objective Type Tests, Term paper and Assignments
B: Pre-Scheduled Test-1: Based on Objective Type & Subjective Type Test (By Enlarged Subjective Type)
C: Pre-Scheduled Test-2: Based on Objective Type & Subjective Type Test (By Enlarged Subjective Type)
D: End-Term Exam (Final): Based on Objective Type Tests
E: Total Marks
L: Lectures T: Tutorial P: Practical Cr: Credits

The following Transaction Modes are used for each subjects:

Modes of classroom transaction

1) Lecture
2) Demonstration
3) Project Method
4) Inquiry training
5) Seminar
6) Group discussion
7) Flipped learning
8) Tutorial
9) Self-learning
10) Case study

The following tools can be used in different transactional modes:

1. PPT
2. Video
3. e-content
4. google drive

Course Code **CST.507**
Course Name **Mathematical Foundation of Computer Science**
Credits **4**

Course Objectives: To understand the mathematical 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: On completion of the course the students should be able to

- To understand the basic notions of discrete and continuous probability.
- To understand the methods of statistical inference, and the role that sampling distributions play in those methods.
- To be able to perform correct and meaningful statistical analyses of simple to moderate complexity.

CONTENTS

Unit 1 **17 hours**

Distribution Function: Probability mass, density, and cumulative distribution functions, Conditional Probability, Expected value,

Applications of the Univariate and Multivariate problems. Probabilistic inequalities, Random samples, sampling distributions of estimators and Maximum Likelihood.

Unit 2 **15 hours**

Statistical inference: Descriptive Statistics**,** Introduction to multivariate statistical models, Multivariate Regression, Multinominal regression and classification problems,

Principal components analysis**,** The problem of over fitting model assessment.

Unit 3 **16 hours**

Graph Theory: Isomorphism, Planar graphs, graph colouring, Hamilton circuits and Euler cycles.

Specialized techniques to solve combinatorial enumeration problems

Unit 4 **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.

Suggested Readings

1. John Vince, Foundation Mathematics for Computer Science, Springer International Publishing, Edition 1, 2015.
2. Kishor S. Trivedi, Probability and Statistics with Reliability, Queuing, and Computer Science Applications. Wiley, Second Edition, Nov 2001, ISBN:978-0-471-33341-8
3. Michel Mitzenmacher and E. Upfal. Probability and Computing: Randomized Algorithms and Probabilistic Analysis, Cambrige University Press, January 31, 2005, ISBN: 978-0521835404
4. Alan Tucker, Applied Combinatorics, Wiley, 6th Edition, Feb 1, 2012, ISBN: 978-0470458389

Course Code **CST.506**
Course Name **Advanced Data Structures and Algorithms**
Credits **4**

Course Objectives:

- The student should be able to choose appropriate data structures, understand the ADT/libraries, and use it to design algorithms for a specific problem.
- Students should be able to understand the necessary mathematical abstraction to solve problems.
- To familiarize students with advanced paradigms and data structure used to solve algorithmic problems.
- Student should be able to come up with analysis of efficiency and proofs of correctness.

Course Outcomes:

After completion of course, students would be able to:

- Understand the implementation of symbol table using hashing techniques.
- Develop and analyze algorithms for red-black trees, and B-trees.
- Develop algorithms for text processing applications.
- Identify suitable data structures and develop algorithms for computational geometry problems.

CONTENTS

Unit 1 **14 hours**

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 2 **16 hours**

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

Design Strategies: Divide-and-conquer, Dynamic Programming, and Greedy Method.

Unit 3 **16 hours**

Text Processing: The naive string-matching algorithm, Rabin-Karp, String matching with finite automaton, 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 4 **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.

Suggested Readings

1. T.H. Cormen, C. E. Leiserson, RL Rivest and C Stein, Introduction to Algorithms, 3rd Edition, MIT Press, Alan Tucker, 2010.
2. Sridhar, S., Design and Analysis of Algorithms. Oxford University Press India, 1st Edition, 2014.
3. Mark Allen Weiss, Data Structures and Algorithm Analysis in C++, 2nd Edition, Pearson, 2004.
4. M T Goodrich, Roberto Tamassia, Algorithm Design, John Wiley, 1st Edition, 2002.
5. Aho, A.V., Hopcroft, J.E. and Ullman, J. D., Data Structures and Algorithms. India: Pearson Education, 2nd Edition, 2009.
6. Horowitz, E., Sahni, S. and Rajasekaran, S., Fundamentals of Computer Algorithms, Galgotia Publications, 2nd Edition, 2010.

Course Code **CBS.506**
Course Name **Ethical Hacking**
Credits **4**

Course Objectives:

- 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.

Course Outcomes:

After completion of course, students would be able to:

- Understand the core concepts related to vulnerabilities and their causes
- Understand ethics behind hacking and vulnerability disclosure
- Appreciate the impact of hacking

- Exploit the vulnerabilities related to computer system and networks using state of the art tools and technologies.

CONTENTS

Unit 1 **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 2 **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 3 **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 4 **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.

Suggested Readings

1. Baloch, R., Ethical Hacking and Penetration Testing Guide, CRC Press, 2015.
2. Beaver, K., Hacking for Dummies, 3rd ed. John Wiley & sons., 2013.
3. Council, Ec. , Computer Forensics: Investigating Network Intrusions and Cybercrime, Cengage Learning, Second Edition, 2010
4. McClure S., Scambray J., and Kurtz G, Hacking Exposed. Tata McGraw-Hill Education, 6the Edition, 2009
5. 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, 2010
6. Davidoff, S. and Ham, J., Network Forensics Tracking Hackers through Cyberspace, Prentice Hall, 2012.
7. Michael G. Solomon, K Rudolph, Ed Tittel, Broom N., and Barrett, D.,Computer, Forensics Jump Start, Willey Publishing, Inc, 2011

Course Code CBS.507
Course Name Intrusion Detection
Credits 4

Course Objectives:

- 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.

Course 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 an enterprise and appropriately apply Intrusion Detection tools and techniques in order to improve their security posture

CONTENTS

Unit 1 **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 2 **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 3 **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 4 **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 zeroday
detection-Insider Threat issues-Taxonomy-Masquerade and Impersonation-Traitors, Decoys and Deception-Future: Collaborative Security

Suggested Readings

1. Peter Szor , The Art of Computer Virus Research and Defense, Symantec Press, 2010, ISBN 0-321-30545-3.
2. Markus Jakobsson and Zulfikar Ramzan, Crimeware, Understanding New Attacks and Defenses, Symantec Press, 2008, ISBN: 978-0-321-50195-0.

Course Code **CBS.508**
Course Name **Data Encryption &Network Security**
Credits **4**

Course Objectives:

This course will cover the concept of security, types of attack experienced, encryption and authentication for deal with attacks, what is **Network Perimeter Security**, **Access Control Lists** and **Virtual Private Networks.**

Course Outcomes:

After completion of course, students would be:

At the end of this course the student will have the knowledge of plaintext, cipher text, RSA and other cryptographic algorithm, Key Distribution, Communication Model, Network Perimeter Security, Access Control Lists and Virtual Private Networks.

CONTENTS

Unit 1 **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 2 **15 hours**

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

Unit 3 **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.
Public Key Cryptography and Message Authentication: Approaches to Message Authentication, SHA-1, MD5, Public-Key Cryptography Principles, RSA, Digital, Signatures, Key Management.

Unit 4 **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).

Suggested Readings

1. Forouzan, B.A., Cryptography & Network Security. Tata McGraw-Hill Education, 2010
2. Kahate, A. Cryptography and Network Security. McGraw-Hill Higher Ed., 2009.
3. Godbole, N., Information Systems Security: Security Management, Metrics, Frameworks and Best Practices. 1st Ed. John Wiley & Sons India, 2009.
4. Riggs, C., Network Perimeter Security: Building Defence In-Depth, AUERBACH, USA, 2005.
5. Northcutt S., Inside Network Perimeter Security, 2nd Ed., Pearson Education, 2005.
6. Stallings, W., Network Security Essentials: applications and standards. 3rd ed. Pearson Education India, 2007.
7. Stallings, W., Cryptography and Network Security: Principles and Practice. 6th ed. Pearson, 2004.
8. Kim. D., and Solution, M.G., Fundamentals of Information System Security. Jones & Bartlett Learning, 2010.

Course Code **CBS.509**
Course Name **Information Theory**
Credits **4**

Course Objectives:
The objective of this course is to provide an insight to information coding techniques, error correction mechanism. Various compression techniques for text, video and image are covered for thorough knowledge of efficient information conveying systems.

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

- The aim of this course is to introduce the principles and applications of information theory.
- The course will study how information is measured in terms of probability and entropy.
- The students learn coding schemes, including error correcting codes, The Fourier perspective; and extensions to wavelets, complexity, compression, and efficient coding of audio-visual information.

CONTENTS

Unit 1 **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 2 **14 hours**

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

Unit 3 **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 4 **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

Suggested Readings

1. Fundamentals in information theory and coding, Monica Borda,Springer.
2. Communication Systems: Analog and digital, Singh and Sapre, TataMcGraw Hill.
3. Multimedia Communications Fred Halsall.
4. Information Theory, Coding and Cryptography R Bose.

5. Multimedia system Design Prabhat K Andleigh and Kiran Thakrar.

Course Code CST.508
Course Name Machine Learning
Credits 4

Course Objectives:

- To 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 Deep learning technique and various feature extraction strategies.

Course 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.

CONTENTS

Unit 1 **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 2 **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 3 **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

Unit 4 **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.

Suggested Readings

1. Kevin Murphy, Machine Learning: A Probabilistic Perspective, MIT Press, 2012
2. Trevor Hastie, Robert Tibshirani, Jerome Friedman, The Elements of Statistical Learning, Springer 2009 (freely available online)
3. Christopher Bishop, Pattern Recognition and Machine Learning, Springer, 2007.

Course Code **CST. 514**
Course Name **Research Methodology & IPR**
Credits **4**

CONTENTS

Unit 1 **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 2 **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 3 **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 4 **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 etc. Traditional knowledge Case Studies.

Suggested Readings

1. Stuart Melville and Wayne Goddard, "Research methodology: an introduction for science & engineering students'"
2. Wayne Goddard and Stuart Melville, "Research Methodology: An Introduction"
3. Ranjit Kumar, 2 nd Edition , "Research Methodology: A Step by Step Guide for beginners"
4. Halbert, "Resisting Intellectual Property", Taylor & Francis Ltd ,2007.
5. Mayall , "Industrial Design", McGraw Hill, 1992.
6. Niebel , "Product Design", McGraw Hill, 1974.
7. Asimov , "Introduction to Design", Prentice Hall, 1962.
8. Robert P. Merges, Peter S. Menell, Mark A. Lemley, " Intellectual Property in New Technological Age", 2016.
9. T. Ramappa, "Intellectual Property Rights Under WTO", S. Chand, 2008

Course Code **CST.515**
Course Name **Advanced Data Structure – Lab**
Credits

List of Practical based on:
Lab Evaluation:

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

Evaluation Parameters	**Marks**
Practical File	5
Implementation	15
Viva-voce	30
Total	**50**

Course Code **CBS.510**
Course Name **Ethical Hacking Lab**
Credits

List of Practical based on:
Lab Evaluation:

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

Evaluation Parameters	Marks
Practical File	5
Implementation	15
Viva-voce	30
Total	**50**

Course Code **CBS.511**
Course Name **Intrusion Detection Lab**
Credits

List of Practical based on:

Lab Evaluation:

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

Evaluation Parameters	Marks
Practical File	5
Implementation	15
Viva-voce	30
Total	**50**

Semester –II

Course Code **CST-521**
Course Name **Advance Algorithm**
Credits **4**

CONTENTS

Unit 1 **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 2 **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 3 **15 hours**

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

Unit 4 **16 hours**

One or more of the following topics based on time and interest
Approximation algorithms, Randomized Algorithms, Interior Point Method,

Recent Trands in problem solving paradigms using recent searching and sorting techniques by applying recently proposed data structures.

Suggested Readings

1. "Introduction to Algorithms" by Cormen, Leiserson, Rivest, Stein.
2. "The Design and Analysis of Computer Algorithms" by Aho, Hopcroft, Ullman.
3. "Algorithm Design" by Kleinberg and Tardos.

Course Code **CST.522**
Course Name **Soft Computing**
Credits **4**

Course Objectives:

- To introduce soft computing concepts and techniques and foster their abilities in designing appropriate technique for a given scenario.
- To implement soft computing based solutions for real-world problems.
- 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 on MATLAB to implement various strategies.

Course 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.

CONTENTS

Unit 1 **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, and Learning Neural Networks.

Unit 2 **14 hours**

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

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

Unit 3 **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.

Matlab/Python Lib: Introduction to Matlab/Python, Arrays and array operations, Functions and Files.

Unit 4 **14 hours**

Study of neural network toolbox and fuzzy logic toolbox, Simple implementation of Artificial Neural Network and Fuzzy Logic.
Recent Trands in deep learning, various classifiers, neural networks and genetic algorithms.
Implementation of recently proposed soft computing techniques.

Suggested Readings

1. Jyh:Shing Roger Jang, Chuen:Tsai Sun, EijiMizutani, Neuro:Fuzzy and Soft Computing, Prentice:Hall of India, 2003.
2. George J. Klir and Bo Yuan, Fuzzy Sets and Fuzzy Logic:Theory and Applications, Prentice Hall, 1995.
3. MATLAB Toolkit Manual
4. Ross J.T., (2009). Fuzzy Logic with Engineering Applications John Wiley & Sons.
5. Rajasekaran, S.Vijayalakshmi Pai, G.A. (2003). Neural Networks, Fuzzy Logic and Genetic Algorithms PHI Learning.

7. Priddy L.K., Keller E.P., (2005). Artificial Neural Networks: An Introduction SPIE Press.
8. Gen, M. Cheng, R. (2000). Genetic Algorithms and Engineering Optimization John Wiley & Sons.

Course Code **CBS.521**
Course Name **Malware Analysis & Reverse Engineering**
Credits **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.

Course Outcomes
On completion of the course the student should be able to

- To understand the concept of malware and reverse engineering.
- Implement tools and techniques of malware analysis.

CONTENTS

Unit 1 **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 2 **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 3 **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 4 **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

Suggested Readings

1. Michael Sikorski, Andrew Honig "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" publisher Williampollock

Course Code **CBS-522**
Course Name **Steganography**
Credits **4**

Course Objectives:

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

Course Outcomes

After completion of course, students would be:

- Learn the concept of information hiding.
- Survey of current techniques of steganography and learn how to detect and extract hidden information.
- Learn watermarking techniques and through examples understand the concept.

CONTENTS

Unit 1 **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 2 **12 hours**

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

Unit 3 **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 4 **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.

Suggested Readings

1. Peter Wayner, "Disappearing Cryptography–Information Hiding: Steganography &
2. Watermarking", Morgan Kaufmann Publishers, New York, 2002.
3. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, TonKalker, "Digital
4. Watermarking and Steganography", Margan Kaufmann Publishers, New York, 2008.
5. Information Hiding: Steganography and Watermarking-Attacks and Countermeasures by Neil F.
6. Johnson, ZoranDuric, SushilJajodia
7. Information Hiding Techniques for Steganography and Digital Watermarking by Stefan
8. Katzenbeisser, Fabien A. P. Petitcolas

Course Code **CBS-523**
Course Name **Secure Software Design and Enterprise Computing**
Credits **4**

Course Objectives:

- To fix software flaws and bugs in various software.
- 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.

Course Outcomes

After completion of course, students would be able to:

- Differentiate between various software vulnerabilities.
- Software process vulnerabilities for an organization.
- Monitor resources consumption in a software.
- Interrelate security and software development process.

CONTENTS

Unit 1 **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 2 **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 3 **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 4 **15 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.

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.

Course Code **CBS.524**
Course Name **Big Data Analysis and Visualization**
Credits **4**

Course Objectives:
To prepare the data for analysis and develop meaningful Data Visualizations
Course Outcomes
After completion of course, students would be:
Able to extract the data for performing the Analysis.

CONTENTS

Unit 1 **15 hours**

Data Gathering and Preparation: Data formats, parsing and transformation, Scalability and real-time issues, **Data Cleaning:** Consistency checking, Heterogeneous and missing data, Data Transformation and segmentation

Unit 2 **16 hours**

Exploratory Analysis: Descriptive and comparative statistics, Clustering and association, Hypothesis Generation,
Visualization: Designing visualizations, Time series, Geo-located data, Correlations and connections, Hierarchies and networks, interactivity

Unit 3 **15 hours**

Big Data Technology: Fundamental of Big Data Types, Big data Technology Components, Big Data Architecture, Big Data Warehouse, Functional Vs. Procedural Programming Models for Big Data.

Unit 4 **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

Suggested Readings

1. Making sense of Data: A practical Guide to Exploratory Data Analysis and Data Mining, by GlennJ. Myatt
2. Data Analytics Make Accesible By A. Maheshwari, Orilley Publications
3. Lean Analytics: Use Data to Build a Better Startup Faster, by A. Croll and B. Yoskovitz

4. Oreilley Publications, 1 st Edition, 2013

Course Code CBS.525
Course Name Secure Coding
Credits 4

Course Objectives:

- Understand the most frequent programming errors leading to software vulnerabilities.
- Identify and analyse security problems in software.
- Understand and protect against security threats and software vulnerabilities.
- Effectively apply their knowledge to the construction of secure software systems

Course Outcomes

After completion of course, students would be able to:

- Write secure programs and various risk in the softwares.
- Describe various possible security attacks
- Classify various errors that lead to vulnerabilities
- Real time software and vulnerabilities associated with them.

CONTENTS

Unit 1 **16 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 2 **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 3 **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.

Errors and Exceptions: Handling Error with return code, Managing exceptions, Preventing

Resource leaks, Logging and debugging.

Unit 4 **16 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.

Suggested Readings

1. Seacord, R. C. (2013). Secure Coding in C and C++. 2nd edition. Addison Wisley for Software Engineering Institute,
2. Chess, B., and West, J. (2007). Secure Programming with static Analysis. Addison Wisley Software Security Series.
3. Seacord, R. C. (2009). The CERT C Secure Coding Standard. Pearson Education. Howard, M., LeBlanc, D. (2002). Writing Secure Code. 2ndEdition. Pearson Education.

Course Code **CBS.526**
Course Name **Security Assessment & Risk Analysis**
Credits **4**

Course Objectives:

- Describe 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.

Course Outcomes

After completion of course, students would be:

- Capable of recommending contingency strategies including data backup and recovery and alternate site selection for business resumption planning
- Skilled to be able to describe the escalation process from incident to disaster in case of security disaster.
- Capable of Designing a Disaster Recovery Plan for sustained organizational operations.
- Capable of Designing a Business Continuity Plan for sustained organizational operations.

CONTENTS

Unit 1 **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 2 **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 3 **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 4 **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.

Suggested Readings

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

Course Code **CBS.527**
Course Name **Digital Forensics**
Credits **4**

Course Objectives:

- Provides an in-depth study of the rapidly changing and fascinating field of computer forensics.
- Combines both the technical expertise and the knowledge required to investigate, detect and prevent digital crimes.
- Knowledge on digital forensics legislations, digital crime, forensics processes and procedures, data acquisition and validation, e-discovery tools
- E-evidence collection and preservation, investigating operating systems and file systems, network forensics, art of steganography and mobile device forensics

Course Outcomes:

After completion of course, students would be able to:

- Understand relevant legislation and codes of ethics
- Computer forensics and digital detective and various processes, policies and procedures
- E-discovery, guidelines and standards, E-evidence, tools and environment.
- Email and web forensics and network forensics

CONTENTS

Unit 1 **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 2 **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 3 **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 4 **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

Suggested Readings

1. John Sammons, The Basics of Digital Forensics, Elsevier
2. Davidoff, S. and Ham, J. (2012). Network Forensics Tracking Hackers through Cyberspace, Prentice Hall.
3. Michael G. Solomon , K Rudolph, Ed Tittel, Broom N., and Barrett, D. (2011),Computer Forensics Jump Start, Willey Publishing, Inc.
4. Marcella, Albert J., Cyber forensics: A field mannual for collecting, examining and preserving evidence of computer crimes(2008), New York, Auerbach publications, 2008
5. Davidoff, Sherri, Network forensics: Tracking hackers through cyberspace (2017), Pearson education India private limited.

Course Code **CBS.528**
Course Name **Python Programming for Security Professionals**
Credits **4**

Course Objectives:

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

Course Outcomes:

After completion of course, students would be able to:

- Understand basics python programming
- Use 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

CONTENTS

Unit 1 **13 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, if-else, for, while, range function, continue, pass, break. Strings: Sequence operations, String Methods, Pattern Matching.

Unit 2 **14 hours**

Lists: Basic Operations, Iteration, Indexing, Slicing and Matrixes; Dictionaries: Basic dictionary operations; Tuples and Files; 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 3 **15 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.

Unit 4 **18 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

Suggested Readings

1 . Lutz Mark, (2009). 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(2013), Elsevier.

3. Seitz Justin , (2009). Gray Hat Python: Python Programming with Hackers and Reverse Engineers, Latest Edition, No Starch Press, Inc.

4. Seitz Justin , (2015). Black Hat Python: Python Programming for Hackers and Pentesters, Latest Edition, No Starch Press, Inc

5. Berry Paul, (2011). Head First Python. Latest Edition, O'REILLY Media, Inc.

Course Code **CST. 524**
Course Name **IOT (Internet of Things)**
Credits **4**

Course Objectives:

The objective of this course is to introduce students to the use of Devices in IoT Technology, Real World IoT Design Constraints, Industrial Automation and Commercial Building Automation in IoT.

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

Understand the concepts of Internet of Things

- • Building state of the art architecture in IoT.
- • Design IoT applications in different domain and be able to analyze their performance
- • Implement basic IoT applications on embedded platform

CONTENTS

Unit 1 **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 2 **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 3 **15 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 4 **16 hours**

Developing IoTs: Introduction to Python, Introduction to different IoT tools, Developing applications through IoT tools, Developing sensor based application through embedded system platform, Implementing IoT concepts with python

Text books:

1. Vijay Madisetti, Arshdeep Bahga, "Internet of Things: A Hands-On Approach"
2. Waltenegus Dargie,Christian Poellabauer, "Fundamentals of Wireless Sensor Networks: Theory and Practice
3. Francis daCosta, "Rethinking the Internet of Things: A Scalable Approach to Connecting Everything", 1st Edition, Apress Publications, 2013

Suggested Readings:

1. 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", 1st Edition, Academic Press, 2014.

Course Code **CST-527**
Course Name **Soft Computing – Lab**
Credits

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:

Evaluation Parameters	**Marks**
Practical File	5
Implementation	15
Viva-voce	30
Total	**50**

Course Code **CST-528**
Course Name **Python Programming for Security Professionals – Lab**
Credits

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:

Evaluation Parameters	**Marks**
Practical File	5
Implementation	15
Viva-voce	30
Total	**50**

Semester- III

Course Code **CBS.551**
Course Name **Biometric Security**
Credits **4**

Course Objectives:
The objective of this course is to
- Introduce Bio-metric and traditional authentication methods.
- Describe the background theory of image processing required in biometric security
- Classify algorithms related to various biometrics
- Evaluate the performance of various biometric systems

Course Outcomes:
After completion of course, students would be:
- Perform R&D on bio-metrics methods and systems.
- A good understanding of the various modules constituting a bio-metric system.
- Familiarity with different bio-metric traits and to appreciate their relative significance.
- A good knowledge of the feature sets used to represent some of the popular bio-metric traits.
- Evaluate and design security systems incorporating bio-metrics.
- Recognize the challenges and limitations associated with bio-metrics.

CONTENTS

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.

Suggested Readings

1. Biometrics for network security, Paul Reid, Hand book of Pearson
2. D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition,
   Springer Verlag, 2003.
3. A. K. Jain, R. Bolle, S. Pankanti (Eds.), BIOMETRICS: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999.
4. J. Wayman, A.K. Jain, D. Maltoni, and D. Maio (Eds.), Biometric Systems: Technology,
5. Design and Performance Evaluation, Springer, 2004.
6. Anil Jain, Arun A. Ross, Karthik Nanda kumar, Introduction to biometric, Springer, 2011.
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. (2009). Digital Image Processing. 2nd ed. India: Person Education.

Course Code **CST-552**
Course Name **Data Warehousing and Data Mining**
Credits **4**

Course Objectives:

The objective of this course is to introduce data warehousing and mining techniques. Application of data mining in web mining, pattern matching and cluster analysis is included to aware students of broad data mining areas.

Course Outcomes

After completion of course, students would be:

- Study of different sequential pattern algorithms
- Study the technique to extract patterns from time series data and it application in real world.
- Can extend the Graph mining algorithms to Web mining

- Help in identifying the computing framework for Big Data

CONTENTS

Unit 1 **14 hours**

Introduction to Data Warehousing: Data warehousing Architecture, OLAP Server, Data Warehouse Implementation.

Unit 2 **15 hours**

Data Mining: Mining frequent patterns, association and correlations; Sequential Pattern Mining concepts, primitives, scalable methods;
Classification and prediction; Cluster Analysis – Types of Data in Cluster Analysis, Partitioning methods, Hierarchical Methods; Transactional Patterns and other temporal based frequent patterns,

Unit 3 **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 4 **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

Suggested Readings

1. Jiawei Han and M Kamber, Data Mining Concepts and Techniques, Second Edition, Elsevier Publication, 2011.
2. Vipin Kumar, Introduction to Data Mining - Pang-Ning Tan, Michael Steinbach, Addison Wesley, 2006.
3. G Dong and J Pei, Sequence Data Mining, Springer, 2007.

Course Code **CST-553**
Course Name **Introduction to Intelligent System**
Credits **4**

Course Objectives:

The aim of the course is to introduce to the field of Artificial Intelligence (AI) with emphasis on its use to solve real world problems for which solutions are difficult to express using the traditional algorithmic approach. It explores the essential theory behind methodologies for developing systems that demonstrate intelligent behaviour including dealing with uncertainty, earning from experience and following problem solving strategies found in nature.

Course Outcomes

Able to Demonstrate knowledge of the fundamental principles of intelligent systems and would be able to analyse and compare the relative merits of a variety of AI problem solving techniques.

CONTENTS

Unit 1 **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.

Unit 2 **14 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. Optimisation and search such as stochastic annealing and genetic algorithm.

Unit 3 **16 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 4 **14 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.
Recent trends in Fuzzy logic, Knowledge Representation.

Suggested Readings

1. Luger G.F. and Stubblefield W.A. (2008). Artificial Intelligence: Structures and strategies for Complex Problem Solving. Addison Wesley, 6th edition.
2. Russell S. and Norvig P. (2009). Artificial Intelligence: A Modern Approach. Prentice-Hall, 3rd edition.

Course Code **CST-554**
Course Name **Mobile Applications & Services**
Credits **4**

Course Objectives:

- This course presents the three main mobile platforms and their ecosystems, namely Android, iOS, and PhoneGap/WebOS.

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

Course Outcomes

- On completion of the course the student should be able to identify the target platform and users and be able to define and sketch a mobile application
- understand 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)

CONTENTS

Unit 1 **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 2 **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 3 **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 4 **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 inCommunication protocols for IOT nodes, mobile computimng techniques in IOT, agents based communications in IOT

Suggested Readings

1. Wei-Meng Lee, Beginning AndroidTM 4 Application Development, 2012 by John Wiley & Sons

Course Code **CBS.552**
Course Name **Cyber threat Intelligence**
Credits **4**

Course objective

- By understanding the myriad cyber threats and actor motivations, leader guide organizations in accurately accessing threats, risks, and vulnerabiliti minimize the potential for incidents and, when necessary, provide more thou responses

Course Outcomes

After completion of course, students would be:

- Study of different Cyber Threat
- Study the technique to Develop Cyber Threat Intelligence Requirements.
- Can Collect Cyber Threat Information
- Help in Analyzing and Disseminating Cyber Threat Intelligence

CONTENTS

Unit 1 **15 hours**

Defning 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 Defned, Key Characteristics: Adversary based, Risk focused, Process oriented, Tailored for diverse consumers, The Benefts of Cyber Threat Intelligence

Unit 2 **14 hours**

Developing Cyber Threat Intelligence Requirements : Assets That Must Be Prioritized: Personal information, Intellectual property, Confdential 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 3 **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 4 **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.

Suggested Readings

1. Jon Friedman. Mark Bouchard, CISSP. Foreword by John P. Watters. (2015) Cyber Threat Intelligence.Definitive GuideTM.

Course Code **CST. 555**
Course Name **Operations Research**
Credits **4**

Course Outcomes:

At the end of the course, the student should be able to
Students should able to apply the dynamic programming to solve problems of discreet and continuous variables.
Students should able to apply the concept of non-linear programming
Students should able to carry out sensitivity analysis
Student should able to model the real world problem and simulate it.

CONTENTS

Unit 1 **9 hours**

Optimization Techniques, Model Formulation, models, General L.R Formulation, Simplex Techniques, Sensitivity Analysis, Inventory Control Models

Unit 2 **10 hours**

Formulation of a LPP - Graphical solution revised simplex method - duality theory - dual simplex method - sensitivity analysis - parametric programming

Unit 3 **14 hours**

Nonlinear programming problem - Kuhn-Tucker conditions min cost flow problem - max flow problem - CPM/PERT

Unit 4 **15 hours**

Scheduling and sequencing - single server and multiple server models - deterministic inventory models - Probabilistic inventory control models - Geometric Programming.
Competitive Models, Single and Multi-channel Problems, Sequencing Models, Dynamic Programming, Flow in Networks, Elementary Graph Theory, Game Theory Simulation

Suggested Readings

1. H.A. Taha, Operations Research, An Introduction, PHI, 2008
2. H.M. Wagner, Principles of Operations Research, PHI, Delhi, 1982.
3. J.C. Pant, Introduction to Optimisation: Operations Research, Jain Brothers, Delhi, 2008
4. Hitler Libermann Operations Research: McGraw Hill Pub. 2009
5. Pannerselvam, Operations Research: Prentice Hall of India 2010
6. Harvey M Wagner, Principles of Operations Research: Prentice Hall of India 2010

Course Code **CST.556**
Course Name **Cost Management of Engineering Projects**
Credits **4**

CONTENTS

Unit 1 **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 2 **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 3 **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 4 **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.

Suggested Readings

1. Cost Accounting A Managerial Emphasis, Prentice Hall of India, New Delhi
2. Charles T. Horngren and George Foster, Advanced Management Accounting
3. Robert S Kaplan Anthony A. Alkinson, Management & Cost Accounting
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.

Course Code **CBS.553**
Course Name **Cyber Law**
Credits **4**

Objective: 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.

Course Outcomes: By the end of this Course, students should be able to:

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

CONTENTS

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.

Suggested Readings

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

Course Code **CST.555**
Course Name **Software Metrics**
Credits **4**

Course Objectives:

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

Course Outcomes:

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

- Able to learn role software Metrics in Industry size software
- Empirical investigation of software for a quality measurement.
- Understand and identify software reliability and problem solving by designing and selecting software reliability models.

CONTENTS

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.

Suggested Readings

1. Norman E. Fenton, S. L. P fleeger, "Software Metrics: A Rigorous and Practical Approach", published by International Thomson Computer Press, 2/e, 1998.
2. Stephen H. Kan, "Metrics and Models in Software Quality Engineering", Addison-Wesley Professional, 2/e, 2002.
3. Basu Anirban, "Software Quality Assurance, Testing and Metrics", Prentice Hall India Learning Private Limited, 2015
4. Robert B. Grady, "Practical Software Metrics for Project Management And Process Improvement", Prentice Hall, 1992.
5. Maxwell Katrina D., "Applied Statistics for Software Managers", Prentice Hall PTR, 2002

Course Code **CBS. 600**
Course Name **Dissertation**
Credits **10**

Objectives:

1. 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.

2. 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).

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 on the average of marks given 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	

Evaluation criteria for Mid-Term:

Evaluation Parameter	**Maximum Marks**	**Evaluated By**
Mid Term Review and Presentation	50	**Internal/External Evaluation by Dean of School, HOD/ HOD nominee, Two faculty**

Continuous evaluation	50	**member nominated by Dean/ HOD, Supervisor.**
Total	**100**	

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

Seminar with Minor Project Evaluation:

In this, the student has to select an area and specify the objectives to be achieved.

Evaluation criteria will be based on objective stated and achieved

Timeline Work of Seminar:

Month	**AUG**	**SEP**	**NOV**
Seminar	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

Course Code	**CBS. 600**
Course Name	**Dissertation/Industrial Project**
Credits	

Objective:

In Dissertation the student shall have to carry out the activities/experiments to be completed during Dissertation (as mentioned in the synopsis). The students would present their work to the evaluation Committee (constituted as per the university rules). One research paper (either accepted or published) 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