CENTRAL UNIVERSITY OF PUNJAB BATHINDA

SYLLABUS

M. Tech Computer Science & Engineering
(Cyber Security)

Session - 2025-27

Department of Computer Science & Technology

Central University of Punjab, VPO-Ghudda, Bathinda, Punjab,
India- 151401

Programme Educational Objectives

PEO1: To build a rich intellectual potential embedded with inter-disciplinary knowledge, human values and professional ethics among the youth, aspirant of becoming technologists, so that they contribute to society and create a niche for a successful career.
PEO1: To enable students to gain research and development competence to sustain in academia as well as industry.
PEO1: To Produce "Creators of Innovative Technology".

Graduate Attributes:

After the Completion of Graduate Program student will be able:

1.To demonstrate competence in engineering mathematics, engineering fundamentals, and specialized engineering knowledge appropriate to the program.

2.To acquire appropriate knowledge and skills to identify, formulate, analyze, and solve computer engineering problems in order to reach substantiated conclusion.

3.To conduct investigations of problems by appropriate experiments, analysis and interpretation of data and synthesis of information in order to reach valid conclusions.

4.To design solutions for open-ended engineering problems for designing systems, components or processes that meet specified needs of program.

5.To create, select, apply, adapt, and extend appropriate techniques, resources, and modern engineering tools for a range of engineering activities.

6.To work effectively as a member and leader in teams, preferably in a multi-disciplinary setting.

7.To understand the role of engineer with professional and ethical responsibilities in the society for public interest.

8.To analyze social and environmental aspects of engineering activities.

9.To communicate complex engineering concepts within the profession and with society at large.

10.To appropriately incorporate economics and business practices including project, risk, and change management into the practice of engineering and to understand their limitations.

11.To identify and address their own educational needs in a changing world in ways sufficient to maintain their competence and advancements in future.

12.To apply professional ethics, accountability and equity.

Program Outcome

After the completion of degree program student will be able:

1 To apply mathematical foundations, algorithmic principles, and computer science theory in the modelling and design of security-based systems.

2.To apply the engineering knowledge in all domains, viz., Code security, Network Security, Program security, OS Security etc.

3. To design and conduct experiments as well as to analyze and interpret data for cyber security.

4.To analyze the problem, subdivide into smaller tasks with well-defined interface for interaction among security components, and complete within the specified time frame.

5.To propose original ideas and solutions, culminating into a modern, easy to use tool, by a larger section of the security professionals with longevity.

Course Structure of M.Tech CSE (Cyber Security)

SEMESTER-I

Course Code	Course Title	Course Type	Credit Hours			
			L	T	P	Cr
CST.606	Research Methodology and IPR (SDG-4)	Core	4	0	0	4
CBS.513	Mathematical and Statistical Foundation of Computer Science (SDG-4,9 & 17)	Core	4	0	0	4
Elective I(Opt Any One)						
CBS.507	Intrusion Detection System	Elective/ MOOC course list approved by the department/Skill Development	4	0	0	4
CBS.606	Cryptography					
CBS.607	Python Programming for Cyber Security					
Elective II(Opt Any One)						
CBS.509	Information Theory	Elective/ MOOC course list approved by the department	4	0	0	4
CBS. 514	Number Theory					
CBS.506	Ethical Hacking					
CBS.608	Linux OS and Scripting					
CBS.512	Advanced Data Structures and Algorithms	Foundation	4	0	0	4
XXX.YYY	Any IDC Course offered by other Dept in University or from the list of MOOC Courses approved by the Dept./University	IDC	2	0	0	2
CBS.515	Advanced Data Structures and Algorithms – Lab	Skill Development	0	0	2	1
Elective Lab I (Opt any one)						
CBS.511	Intrusion Detection System Lab	Skill Development	0	0	2	1
CBS.509	Python Programming for Cyber Security –Lab					
CBS.610	Cryptography – Lab					
Elective Lab II(Opt Any One)						
CBS.510	Ethical Hacking-Lab	Skill Development	0	0	2	1
CBS.516	Information Theory-Lab					
CBS.517	Number Theory-Lab					
CBS.611	Linux OS and Scripting – Lab					
Total Credits			**22**	**0**	**6**	**25**

List of IDC for other departments (Semester-I)

Course Code	**Course Title**	**Course Type**	**Credit Hours**			
			L	**T**	**P**	**Cr**
CBS.518	IT Fundamentals	Interdisciplinary courses offered by CST Faculty (For students of other Departments)	2	0	0	**2**
CBS.519	Programming in C					
CST.530	Introduction to Digital Logic					
CST.531	Multimedia and its Applications					
CST.532	Introduction to MatLab					
CST.607	Basics of Python Programming					
Total Credits			**2**	**0**	**0**	**2**

Course Structure of M.Tech CSE (Cyber Security)

SEMESTER-II

Course Code	Course Title	Course Type	Credit Hours			
			L	T	P	Cr
CST.508	Machine Learning	Core	4	0	0	**4**
CBS.540	Multimedia security	Core	4	0	0	**4**
Elective III(Opt Any One)						
CBS.521	Malware Analysis & Reverse Engineering	Elective/ MOOC course list approved by the department	4	0	0	**4**
CBS.523	Secure Software Design & Enterprise Computing					
CBS.524	Big Data Analytics and Visualization					
CST.524	Internet of Things					
CBS.621	Web development and penetration testing					
Elective IV(Opt Any One)						
CBS.527	Digital Forensics	Elective/ MOOC course list approved by the department	4	0	0	**4**
CBS.525	Secure Coding					
CBS.622	Hardware Security					
CST.529	Blockchain Technology (SDG 1,2,3,8,9,12,16 & 17)					
CBS.530	Quantum Computing & Cryptography					
CBS.623	Network security	Skill Development	4	0	0	4
XXX.YYY	Any VAC Course offered by the University or from the list of MOOC Courses approved by the Dept./University	Value Aided either as Theory* or Practical**	2	0	4	**2**
CBS.624	Multimedia security – Lab	Skill Development	0	0	2	**1**
CBS.625	Network Security – Lab	Skill Development	0	0	2	**1**
Elective Lab III(Opt Any One)						
CBS.531	Malware Analysis & Reverse Engineering Lab	Skill Development	0	0	2	**1**
CBS.533	Secure Software Design & Enterprise Computing Lab					
CBS.534	Big Data Analytics and Visualization Lab					
CST.534	Internet of Things-Lab					
CBS. 626	Web development and penetration testing– Lab					
Elective Lab IV(Opt Any One)						
CBS.535	Digital Forensics Lab	Skill Development	0	0	2	**1**
CBS.536	Secure Coding Lab					
CBS.627	Hardware Security – Lab					
CST.536	Blockchain Technology Lab (SDG 1,2,3,8,9,12,16 & 17)					

CBS.538	Quantum Computing & Cryptography Lab					
CST.517	Machine Learning Lab	Skill development	0	0	2	1
Total Credits			**22**	**0**	**4**	**27**

List of Value Added Courses (Semester II)

Course Code	Course Title	Course Type	Credit Hours			
			L	T	P	Cr
CST.504	Basics of Machine Learning*	Value added Course	2	0	0	**2**
CBS.504	Report Writing using LaTeX	Value added Course	2	0	0	**2**
CST. XXX	AI for Education	Value added Course	2	0	0	**2**

*** For other departments only**

Course Structure of M.Tech CSE (Cyber Security)

SEMESTER-III

Course Code	Course Title	Course Type	Credit Hours			Credits
			L	T	P	
CBS.551	Biometric Security	**Opt Any one** Discipline Elective/ MOOC course list approved by the department	3	0	2	**4**
CST.552	Data Warehousing and Data Mining					
CBS.526	Security Auditing and Risk Management					
CST.554	Mobile security and services					
CBS.632	Deep learning					
CBS.552	Cyber Threat Intelligence	**Opt Any one** Open Elective/ MOOC course list approved by the department	4	0	0	**4**
CST.556	Cost Management of Engineering Projects					
CBS.553	Cyber Law					
CST.557	Software Metrics					
CBS.600	*Dissertation Part I	Core	0	0	20	**10**
Total Credits			**8**	**0**	**24**	**19**

*Students will have an option to go for an Industrial Project. Students going for Industrial Project will complete the theory courses of the semester through MOOCs/Swayam/NPTEL Portal

Course Structure of M.Tech CSE (Cyber Security)

SEMESTER- IV

Course Code	Course Title	Course Type	Credit Hours			
			L	**T**	**P**	**Cr**
CBS.600	Dissertation Part II	Core	0	0	32	**16**
Total Credits			**0**	**0**	**32**	**16**

Mode of Transaction: Lecture, Laboratory based Practical, Seminar, Group discussion, Team teaching, Self-learning.

Evaluation Criteria for Theory Courses/or As per University Pattern

A. Continuous Assessment/Internal Assessment: [25 Marks]
B. Mid Semester Test: Based on Subjective Type Test [25 Marks]
C. End Semester Test: Based on Subjective Type Test(70%) and Objective(30%) [50 Marks]

*Every student has to take up one ID courses of 02 credits from other disciplines in semester I of the program and Value Added Course of 2 credits in Semester II.

SEMESTER – I

Course Code: CST.606
Course Title: Research Methodology and IPR
Total Hours: 60

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

Course Learning Outcomes:
After completion of course, students would be able to:
CLO1: Explain effective methods to formulate a research problem.
CLO2: Analyze research related information and follow research ethics.
CLO3: Apply intellectual property law principles (including copyright, patents, designs and trademarks) to practical problems and be able to analyse the social impact of IPR.

Units/Hours	Contents	Mapping with Course Learning Outcome
I **15 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.	**CLO1**
	Activities: Assignment based learning	
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.	**CLO2**
	Activities: Exercise based learning and practical hands on training	
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	**CLO3**
	Activities: Case Studies	

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.	**CLO3**
	Activities: Group discussion	

Transactional Modes:

- Lecture
- Case Studies
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Melville, S. and Goddard, W. (1996). Research methodology: An introduction for science & engineering students. South Africa: Juta Academic.
2. Goddard, W. and Melville, S. (2001). Research Methodology: An Introduction. South Africa: Juta Academic.
3. Kumar, R. (2019). Research Methodology: A Step by Step Guide for beginners. New Delhi: SAGE Publications Ltd.
4. Halbert, (2006). Resisting Intellectual Property. New Delhi: Taylor & Francis Ltd.
5. Mayall, (2011). Industrial Design. New Delhi: McGraw Hill.
6. Niebel, (1974). Product Design. New Delhi: McGraw Hill.
7. Asimov, M. (1976). Introduction to Design. United States: Prentice Hall.
8. Merges, R. P., Menell, P. S., and Lemley, M. A. (2003). Intellectual Property in New Technological Age. United States: Aspen Law & Business.
9. Flick, U. (2011). Introducing research methodology: A beginner's guide to doing a research project. New Delhi: Sage Publications India.
   Research Articles from SCI & Scopus indexed Journals.

Course Code: CBS.513
Course Title: Mathematical and Statistical Foundation of Computer Science
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:
To make students 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, Bioinformatics, Machine learning. To develop the understanding of the mathematical and logical basis to many modern techniques in information technology like machine learning, programming language design, and concurrency.

Course Learning Outcomes:
After completion of course, students would be able to:
CLO1:Describe the basic notions of discrete and continuous probability.
CLO2:Explain methods of statistical inference and understand the role of sampling distributions.
CLO3:Apply statistical analyses to solve problems of moderate complexity.
CLO4: Categorize mathematical models for various domain-specific analyses.

Units/Hours	**Contents**	**Mapping with Course Learning Outcome**
I **15 Hours**	**Fundamentals of Probability and Distributions :** Probability Mass and Density Functions Cumulative Distribution Functions (CDF) Common Probability Distributions: Binomial, Poisson, and Normal Expected Value, Variance, and Probabilistic Inequalities Kurtosis and Skewness	**CLO1**
	Activities: Exercise-based learning with practical examples.	
II **15 Hours**	**Sampling Distributions, Point Estimation, and Statistical Inference** Unbiased Estimators, Variance of Estimators, and Standard Error, Methods of Point Estimation: Method of Moments, Method of Maximum Likelihood, Bayesian Estimation, Tests on the Mean of Single and Two Sample Normal Distributions (Known and Unknown Variance), Non-parametric Tests for Difference in Two Means	**CLO1, CLO2**
	Activities: Analysis of live data from dataworld.org/Kaggle.com.Application of statistical methods to sample data.	
III **15 Hours**	**Statistical Methods and Graph Theory** Basic Statistics: Measures of Central Tendency (Mean, Median, Mode) and Dispersion (Variance, Standard Deviation, Standard Error), Parametric vs Non-parametric Statistics, One-	**CLO2, CLO3**

	Way and Two-Way Analysis of Variance (ANOVA), Introduction to Fuzzy Set Theory, Graph Theory: Isomorphism, Planar Graphs, Graph Coloring, Hamilton Circuits, Euler Cycles	
	Activities: Simulation based learning from web resources, Statistical analysis of real-world datasets (e.g., Kaggle) and graph theory exercises.	
IV **15 Hours**	**R Programming and Applications in Computer Science** Introduction to R Programming, Functions, Control Flow, and Loops, Working with Vectors, Matrices, and Data Files, Statistical and Mathematical Operations in R, Applications in Data Mining, Machine Learning, Computer Security, Software Engineering, and Bioinformatics, Recent Trends in Mathematical Models and Distribution Functions in Computer Science (e.g., Soft Computing, Computer Vision)	**CLO3, CLO4**
	Activities: Hands-on exercises using R for statistical analysis and problem-solving in computer science domains.	

Transactional Modes:

- Lecture
- Blended Learning
- Collaborative Learning
- Peer Learning/Teaching
- Online Teaching Tools

Suggested Readings:

1. Vince, J. (2015). Foundation Mathematics for Computer Science. New York: Springer International Publishing.
2. Trivedi, K. S. (2008). Probability and Statistics with Reliability, Queuing, and Computer Science Applications. United states: Wiley.
3. Mitzenmacher, M., & Upfal, E. (2017). Probability and Computing: Randomized Algorithms and Probabilistic Analysis. New Delhi: Cambridge University Press.
4. Tucker, A. (2016). Applied Combinatorics, United State: Wiley.

Research Articles from SCI & Scopus indexed Jour

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

L	T	P	Cr
4	0	0	4

Course Objectives:

This course aims to equip students with the ability to critically compare various tools and approaches for Intrusion Detection through quantitative analysis, enabling them to determine the most effective methods for minimizing security risks. Additionally, students will be able to identify and describe the essential components of intrusion detection systems and evaluate emerging IDS technologies based on the fundamental capabilities shared by all IDS solutions.

Course Learning Outcomes:

After completion of course, students would be able to:

CLO1: 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.

CLO2: Evaluate the security of an enterprise and appropriately apply Intrusion Detection tools and techniques in order to improve their security posture.

Units/Hours	Contents	Mapping with Course Learning Outcome
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. **Activities:** Assignment based and numerical exercise based learning, Case study-based learning of different security mechanisms.	**CLO1**
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. **Activities:** Assignment based and numerical exercise based learning, Case study-based learning of different security mechanisms.	**CLO1**
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 Behaviour Based Anomaly Detectors (rate based)-Host-based Anomaly Detectors-Software Vulnerabilities- State transition, Immunology, Payload Anomaly Detection. **Activities:** Assignment based and numerical exercise based learning, Case study-based learning of different security mechanisms.	**CLO2**

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. **Activities:** Assignment based and numerical exercise based learning, Case study-based learning of different security mechanisms.	**CLO2**

Transactional Modes:

- Lecture
- E-tutorial
- Collaborative Learning
- Peer Learning/Teaching
- Online Teaching Tools

Suggested Readings:

1. Szor, P. (2010). The Art of Computer Virus Research and Defense, United States: Symantec Press.
2. Jakobsson, M., and Ramzan, Z. (2008). Crimeware, Understanding New Attacks and Defenses, United States: Symantec Press.
3. Research Articles from SCI & Scopus indexed Journals.

Course Code: CBS.606
Course Title: Cryptography
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:

The objective of this course is to provide students with a comprehensive understanding of the foundational concepts and mathematical principles underlying cryptography. It aims to develop students' knowledge of the evolving landscape of security, including its needs, trends, services, and techniques. The course will enable learners to analyze and apply classical and modern symmetric cryptographic algorithms, as well as understand the design and operation of asymmetric key cryptography and cryptographic hash functions. Furthermore, students will be equipped to evaluate and compare user authentication mechanisms and explore security implementations across various layers of network architecture, preparing them for advanced study and application in the field of information security.

Course Learning Outcomes:

CLO1: Explain the Mathematics of Cryptography and need, trends, services and techniques of security.
CLO2: Discuss the various Classical Cryptographic and Symmetric Key Cryptography algorithms.
CLO3: Learn the various Asymmetric Key Cryptography and Hash function algorithms.
CLO4: Compare the various User Authentication Mechanisms
CLO5: Describe the security at various layers.

Units/Hours	Contents	Mapping with Course Learning Outcome
Unit-I **15 Hours**	Mathematics of Cryptography- Prime and Composite Numbers, Greatest Common Divisor, Euclidean algorithm, Modulo arithmetic, Fermat's little theorem, Multiplicative Inverse, Euler's theorem and Totient function, Discrete logarithm. Introduction to Security: Need for security, Security Trends, Security Attacks, Security Services, Security Mechanisms. Security techniques: Plaintext, Cipher text, Encryption & Decryption, Cryptanalysis techniques.	**CLO1**
	Activities: Assignment based and numerical exercise based learning, Case study based learning of different security mechanisms.	
Unit-II **15 Hours**	Classical Cryptographic Algorithms: Substitutions techniques- Monoalphabetic ciphers, Polyalphabetic Ciphers, Transposition Techniques, and Cryptanalysis of classical cryptographic algorithms. Symmetric Key Cryptography: Algorithm types & Modes: - Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB) Output Feedback (OPFB) Mode, Counter (CTR) Mode. Morden symmetric key Cryptographic Algorithms: Data	**CLO2**

	Encryption Standard (DES), Triple DES, RC4, IDEA, Advance Encryption Algorithm (AES), Cryptanalysis.	
	Activities: Assignment based and numerical exercise based learning, Implementation of various cryptographic algorithms using computer programming.	
Unit-III **15 Hours**	Asymmetric key Cryptographic Algorithms:- Public-Key Cryptography Principles, Diffie–Hellman key exchange algorithm, Knapsack algorithm, RSA. Message Authentication: Approaches to Message Authentication, MD5, SHA-512, Digital Signature: Comparison, Process, Services, Attacks on Digital Signature, Digital Signature Scheme. User Authentication Mechanism: Authentication basics, Passwords, Authentication tokens, Certificate based & Biometric authentication.	**CLO3** **CLO4**
	Activities: Implementation and web based simulation of various cryptographic algorithms.	
Unit IV **15 Hours**	Security at the Application Layer: Email: E-mail Architecture, E-mail Security, Secure Electronic Transaction, Security at the Transport Layer: Secure Socket Layer (SSL), Transport Layer Security (TLS).	**CLO5**
	Activities: Brainstorming, assignment based learning	

Transactional Modes:

- Lecture
- Blended Learning
- Collaborative Learning
- Case Study
- Online Teaching Tools

Suggested Readings:

1. Kahate, A. (2011). *Cryptography and Network Security*. New Delhi: tata McGraw-Hill Higher Ed.
2. Forouzan, B. A. (2010). Cryptography & Network Security. New Delhi:Tata McGraw-Hill Education.
3. Stallings, W. (2022). *Cryptography and Network Security: Principles and Practice, Global Edition*. Pearson Higher Ed.
4. Nielson, S. J., & Monson, C. K. (2019). *Practical Cryptography in Python: Learning Correct Cryptography by Example*. Apress.
5. Stallings, W. (2014). *Cryptography and Network Security: Principles and Practice, International Edition: Principles and Practice*. Pearson Higher Ed.
6. Kim, D., & Solomon, M. G. (2016). *Fundamentals of Information Systems Security*. Jones & Bartlett Publishers.
7. Stallings, W. (2017b). *Network Security Essentials: Applications and Standards*.
8. Research Articles from SCI & Scopus indexed Journals.

Course Code: CBS.607
Course Title: Python Programming for Cyber Security
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:

The objective of this course is to introduce students to the fundamental concepts of Python programming, enabling them to gain a solid understanding of the language. It provides learners with the opportunity to explore and work with various Python modules, enhancing their coding proficiency. Through hands-on practice and implementation, students will develop the ability to write Python code to perform a wide range of programming tasks effectively.

Course Learning Outcomes:

After completion of course, students would be able to:
CLO1: Use basics python programming constructs and various Python modules required for accessing operating system and Network.
CLO2: Write scripts in Python language for Network related activities.
CLO3: Prepare python scripts to perform activities related to forensics.

Units/Hours	Contents	Mapping with Course Learning Outcome
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.	**CLO1**
	Activities: Implementation and solution of real time problem.	
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.	**CLO1**
	Activities: Assignment based Learning of real time problem.	

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.	**CLO1**
	Activities: Analysis of cyber security related data.	
IV **14 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.	**CLO2** **CLO3**
	Activities: Analysis of real world data from Kaggle.com/dataworld.org website Implementation of various cyber security related tasks.	

Transactional Modes:

- Lecture cum Demonstration
- Peer Learning/Teaching
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Lutz, M. (2013). *Learning Python* (5th ed.). O'Reilly Media.
2. O'Connor, T. J. (2014). *Violent Python: A cookbook for hackers, forensic analysts, penetration testers, and security engineers*. No Starch Press.
3. Poston, H. E. (2020). *Python for cybersecurity: A comprehensive guide to building tools for protecting your network*. Apress.
4. Seitz, J. (2014). *Black Hat Python: Python programming for hackers and pentesters*. No Starch Press.
5. Sweigart, A. (2015). *Automate the boring stuff with Python: Practical programming for total beginners*. No Starch Press.
6. Erickson, J. (2008). *Hacking: The art of exploitation* (2nd ed.). No Starch Press.

Course Code: CBS.509
Course Title: Information Theory
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:

The objective of this course is to provide students with an insightful understanding of information theory and its significance in the field of communication and data processing. It aims to familiarize students with various coding techniques and error correction mechanisms, laying a strong foundation for reliable data transmission. The course also offers students the opportunity to compare and contrast different coding methods, enabling them to critically analyze and select appropriate techniques for specific applications.

Course Learning Outcomes:

After completion of course, students would be able to:
CLO1: Describe the principles and applications of information theory.
CLO2: Demonstrate how information is measured in terms of probability and entropy.
CLO3: Compare coding schemes, including error correcting codes.

Units/Hours	Contents	Mapping with Course Learning Outcome
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.	CLO-1 CLO-2
	Activities: Assignment based and numerical exercise based learning.	
II 15 Hours	Types of codes: block codes, Hamming and Lee metrics, description of linear block codes, parity check Codes, cyclic code, Masking techniques.	CLO-3
	Activities: Assignment based and numerical exercise based learning, Demonstration of above theory using MATLAB tools.	
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.	CLO-3
	Activities: Assignment based and numerical exercise based learning, Demonstration of above theory using MATLAB tools.	

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.	**CLO-3**
	Activities: Assignment based and numerical exercise based learning, Case based learning of different compression algorithms.	

Transactional Modes:

- Lecture
- Blended Learning
- Collaborative Learning
- Peer Learning/Teaching
- Online Teaching Tools

Suggested Readings:

1. Borda, M. (2011). Fundamentals in information theory and coding. New York: Springer.
2. Singh, R. P. and Sapre, S. D. (2007). Communication Systems: Analog and digital. New Delhi: Tata McGraw Hill.
3. Halsall, F. (2001). Multimedia Communications, Addition-Wesley.
4. Bose, R. (2001). Information Theory, Coding and Cryptography. New Delhi: Tata McGraw Hill.
5. Andleigh, P. K. and Thakrar, K. (1996). Multimedia system Design. United States: Prentice Hall PTR.
6. Research Articles from SCI & Scopus indexed Journals.

Course Code: CBS.514
Course Title: Number Theory
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:

The objective of this course is to introduce students to the foundational principles of cryptography and information theory. It aims to develop an understanding of how mathematical concepts are applied in securing data and communications. The course encourages students to explore the interdisciplinary nature of cryptography, fostering an appreciation for its applications in modern research and technology.

Course Learning Outcomes:

After completion of course, students would be able to:
CLO1: Describe the basic concepts of number theory and uses of number theoretic concepts and logics in deep learning of cryptography and cryptographic techniques.
CLO2: Develop mathematical concepts, logics towards solving cryptographic problems and design new or modify existing cryptographic techniques.
CLO3: Solve techniques such as data collections, data analyzing and pattern reorganization etc, and to establish strong relations between mathematics and cyber security techniques.

Units/Hours	**Contents**	**Mapping with Course Learning Outcome**
I **12 Hours**	Number Systems: Natural numbers, Mathematical induction, Recurrence relations, The Division Algorithm, Catalan Numbers, Prime and Composite Numbers, Fibonacci and Fermat Numbers Greatest Common Divisor, Euclidean algorithm, Fundamental theorem of Arithmetic.	**CLO-1**
	Activities: Assignment based and numerical exercise based learning, Demonstration of above theory using Mathematica/MATLAB tools.	
II **14 Hours**	Diophantine equations: Modulo arithmetic, Congruence classes, Modular Exponentiation, Towers of Powers Modulo m, Linear Congruences, Multiplicative inverse.	**CLO-2**
	Activities: Assignment based and numerical exercise based learning, Demonstration of above theory using Mathematica/MATLAB tools.	
III **16 Hours**	Systems of Linear Congruences, Chinese remainder theorem, Wilson’s Theorem, Euler's extended algorithm, Fermat's little theorem, Multiplicative Functions, Totient function, Euler's theorem.	**CLO-3**
	Activities: Assignment based and numerical exercise based learning, Demonstration of above theory using Mathematica/MATLAB tools.	

IV **18 Hours**	Elementary number theory: Prime numbers, Number bases, Primality testing algorithm, Primitive Roots and Indices, The Order of a Positive Integer, discrete logarithm, primitive roots for Primes, Number sieves, The Algebra of Indices, Quadratic Residues.	**CLO-3** **CLO-1**
	Activities: Assignment based and numerical exercise based learning, Demonstration of above theory using Mathematica/MATLAB tools.	

Transactional Modes:

- Lecture cum Demonstration
- Peer Learning/Teaching
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Erickson, M., and Vazzana, A. (2015). Introduction to Number Theory. London: Chapman & Hall/CRC.
2. Koshy, T. (2005). Elementary Number Theory with applications. Elsevier India.
3. Koblitz, N. (1986). Course on Number Theory and Cryptography. New York: Springer Verlag.
4. Research Articles from SCI & Scopus indexed Journals.

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 familiarize students with the fundamental principles of Ethical Hacking, enabling them to understand the methodologies, tools, and techniques used by ethical hackers to identify and address security vulnerabilities. The course aims to build a foundational understanding of cybersecurity from an ethical standpoint, preparing students to apply these techniques responsibly in practical scenarios to enhance system security.

Course Learning Outcomes:

After completion of course, students would be able to:

CLO1: Explain the core concepts related to vulnerabilities and their causes.
CLO2: Discuss ethics behind hacking and vulnerability disclosure.
CLO3: Demonstrate the impact of hacking.
CLO4: Design methods to extract vulnerabilities related to computer system and networks using state of the art tools and technologies.

Units/Hours	Contents	Mapping with Course Learning Outcome
I **13 Hours**	Ethical hacking process, Hackers behaviour & mindset, Maintaining Anonymity, Hacking Methodology, Information Gathering, Active and Passive Sniffing, Spoofing: IP spoofing, MAC Spoofing, DNS spoofing. Physical security vulnerabilities and countermeasures. Internal and External testing. Types of malware (Trojan, virus, worms, etc.), advanced persistent threat and file-less malware. Preparation of Ethical Hacking and Penetration Test Reports and Documents.	**CLO1 and CLO2**
	Activities: Brainstorming, assignment based learning	
II **17 Hours**	Foot Printing and Reconnaissance: Information gathering using advanced search engines, archive.org, netcraft, whois, host, dig, dnsenum and NMAP tool. Google Dorks. Searhing Vulnerabilities using Shodan. Password attack. Denial of service (DoS) attacks and and Distributed DoS (DDoS) attack. Types of DoS attacks, Social Engineering attacks and countermeasures.	**CLO3 and CLO 4**
	Activities: Exercise based learning and practical hands on training	
III **14 Hours**	Network Infrastructure Vulnerabilities: Packet sniffing using Wireshark and Burpsuite, ARP Cache Poisoning attack, Wireless Hacking: Wireless footprint, Wireless scanning and enumeration, Gaining access, (hacking 802.11), WEP, WPA, WPA2, WPA3. Evil Twin Attack, Jamming attacks. firewall, Intrusion Detection System (IDS), and Honeypot evasion techniques	**CLO3** **CLO 4**

	Activities: Exercise based learning and practical hands on training	
IV **16 Hours**	Installing and using Kali Linux Distribution, Introduction to penetration testing tools in Kali Linux. Introduction to Metasploit: Metasploit framework, Metasploit Console, Payloads, Metrpreter, Introduction to Armitage, Attacks using Metasploit framework: Exploiting remote System, privilege escalation, remote code execution, Client-side browser exploits. Exploiting mobile devices. Case Studies of recent vulnerabilities and attacks.	**CLO3 and CLO 4**
	Activities: Exercise based learning and practical hands on training	

Transactional Modes:

- Lecture cum Demonstration
- Blended Learning
- Collaborative Learning
- Experimentation
- Online Teaching Tools

Suggested Readings:

1. Graham D.G. (2021). Ethical Hacking: A Hands-on Introduction to Breaking In. No Starch Press.
2. Baloch, R. (2015). Ethical Hacking and Penetration Testing Guide. London: CRC Press.
3. Stuttard, D., and Pinto, M. (2011). The Web Application Hacker's Handbook. United States: Wiley.
4. Beaver, K. (2013). Hacking for Dummies. United States: John Wiley & sons.
5. Council, Ec. (2010). Computer Forensics: Investigating Network Intrusions and Cybercrime, Cengage Learning.
6. McClure, S., Scambray. J., and Kurtz G. (2009). Hacking Exposed. New Delhi: Tata McGraw-Hill Education.
7. International Council of E-Commerce Consultants. (2010). Penetration Testing Network and Perimeter Testing Ec-Council/ Certified Security Analyst Vol. 3 of Penetration Testing. Massachusetts: Cenage Learning.
8. Davidoff, S., and Ham, J. (2012). Network Forensics Tracking Hackers through Cyberspace, New Delhi: Prentice Hall.
9. Solomon, M.G., Rudolph, K., Tittel, E., Broom N., and Barrett, D. (2011). Computer, Forensics Jump Start. United States: Willey Publishing.
10. Research Articles from SCI & Scopus indexed Journals

Course Code: CBS. 608

Course Title: Linux OS and Scripting

Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:

The objective of this course is to familiarize students with the Linux operating system environment, enabling them to execute standard commands and navigate the Linux interface effectively. The course aims to equip students with the skills required to develop and customize Linux shell programs while utilizing a wide range of standard Linux development and programming tools. Additionally, it focuses on building the necessary competencies for system-level programming, including inter-process and intra-process communication techniques.

Course Learning Outcomes:

CLO1: Understand effective use of linux utilities

CLO2: Describe the basics of shell scripting language.

CLO3: Apply the concepts of control structure, loops, case and functions in shell programming.

CLO4: Design the Real-Life Scripting

Units/Hours	**Contents**	**Mapping with Course Learning Outcome**
Unit 1 **16 Hours**	Linux basics: Creating First Virtual Machine, Linux Installation, basics of linux, basic commands, variables, aliases, advanced commands, using help/wildcards, soft/hard links, backup/restore using tar, mounting/unmounting, stdin/stdout/stderr.	**CLO1**
	Activities: Assignments and Group Discussion.	
Unit-II **14 Hours**	Shell Scripting Basics: Shell Scripting Basics, Kernel, Shell, Shell Scripting, Types of Shells, Starting a Shell, Run a Shell Script. Scripting Standards: Scripting Standards, Scripts Naming Convention, Script File Permissions, Shell Script Format, Sequence of Script Execution.	**CLO2**
	Activities: Brainstorming, assignment-based learning	
Unit-III **14 Hours**	Shell Scripting: First Script - Hello World, Run Basic Tasks - Script, Run Basic Administration Tasks, Defining Variables, Input/Output Script, Conditions/If Else Statements Scripts, Case Statements Script, For-Loop Script, do-while Scripts.	**CLO3**
	Activities: Hands on experience and Brainstorming.	

Unit-IV **16 Hours**	Real Life Scripting: Real Life Scripting, Accessing Data from a File, Check Remote Servers' Connectivity, Script to Delete Old Files, Copy Files to Remote Hosts, User Directory Assignment, Exploitation scripting: Building exploits with Python, Creating Metasploit Exploits.	**CLO4**
	Activities: Hands on experience and Brainstorming.	

Transactional Modes:

- Lecture cum Demonstration
- Peer Learning/Teaching
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Naik, G. S. (2018). *Learning Linux Shell Scripting: Leverage the power of shell scripts to solve real-world problems, 2nd Edition*. Packt Publishing Ltd.
2. Robbins, A., Beebe, N. H. F. (2005). Classic Shell Scripting: Hidden Commands that Unlock the Power of Unix. Germany: O'Reilly Media, Incorporated.
3. Shotts, W. (2012). The Linux command line: a complete introduction. In *No Starch Press eBooks*. http://ci.nii.ac.jp/ncid/BB11395808
4. Cannon, J. (2015). *Shell Scripting: How to Automate Command Line Tasks Using Bash Scripting and Shell Programming*. CreateSpace.

Course Code: CBS.512
Course Title: Advanced Data Structures and Algorithms
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:
The outcome of this course is to provide the in-depth knowledge of different advance data structures. 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.

Course Learning Outcomes:
After completion of course, students would be able to:
CLO1: Describe various types of Advance data structures and list their strengths and weaknesses.
CLO2: Classify non-randomized and randomized data structures.
CLO3: Design and analyse algorithms using appropriate data structures for real-world problems, i.e., pattern matching and security.
CLO4: Summarize suitable data structure for computational geometry problems.

Units/Hours	**Contents**	**Mapping with Course Learning Outcome**
Unit 1 **15 Hours**	Introduction to Basic Data Structures: Importance and need of good data structures and algorithms. **Hashing:** Review of Hashing, Hash Function, Collision Resolution Techniques in Hashing, Separate Chaining, Open Addressing, Introduction to Hash Tables, Linear Probing, Quadratic Probing, Double Hashing, Rehashing, Extendible Hashing. **Bloom Filter:** Introduction to Bloom Filters, Working of Bloom Filter, Applications of Bloom Filters	**CLO1, CLO3**
	Learning Activities: Implementation and solution of algorithms, Exercise based learning	
Unit-II **15 Hours**	**Skip Lists:** Need for Randomizing Data Structures and Algorithms, Search and Update Operations on Skip Lists, Probabilistic Analysis of Skip Lists, Deterministic Skip Lists. Binary Search Trees, AVL Trees, Red Black Trees, 2-3 Trees, Splay Trees.	**CLO2, CLO3**
	Learning Activities: Visual Modelling Of Data structure.	

Unit-III **15 Hours**	**Advanced String-Matching Algorithms:** Naïve string-matching algorithm, Rabin-Karp algorithm, String matching with finite automata, Knuth-Morris-Pratt algorithm. Standard Tries, Compressed Tries, Suffix Tries. Data Structures for Cryptographic Algorithms: Merkle trees, Bit Array, Circular Buffers, Priority Queues, Message Digest in Information security	**CLO3**
	Activities: Implementation of algorithms and assignment based learning.	
Unit-IV **15 Hours**	**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. One or more of the following topics based on time and interest Approximation algorithms, Randomized Algorithms, Interior Point Method.	**CLO4**
	Activities: Implementation and solution of algorithms, case study of recent algorithm trends.	

Transactional Modes:

- Lecture
- Blended Learning
- Collaborative Learning
- Peer Learning/Teaching
- Online Teaching Tools

Suggested Readings:

1. Cormen, T.H., Leiserson, C. E., Rivest, R.L., and Stein, C. (2022). Introduction to Algorithms. New Delhi: PHI Learning Private Limited.
2. Sridhar, S. (2014). Design and Analysis of Algorithms. New Delhi: Oxford University Press India.
3. Allen Weiss M. (2014). Data Structures and Algorithm Analysis in C++. New Delhi: Pearson Education.
4. Goodrich M.T., Tamassia, R. (2014). Algorithm Design. United States: Wiley.
5. Aho, A.V., Hopcroft, J.E. and Ullman, J.D. (2013). Data Structures and Algorithms. New Delhi: Pearson Education.
6. Horowitz, E., Sahni, S. and Rajasekaran, S. (2017). Fundamentals of Computer Algorithms. New Delhi: Galgotia Publications.
7. Benoit, Anne, Robert, Yves, Vivien and Frederic. (2014). A guide to algorithm design: Paradigms, methods and complexity analysis. London: CRC Press Taylor & Francis group.
8. Research Articles from SCI & Scopus indexed Journals

Course Code: CBS.515
Course Title: Advanced Data Structures and Algorithms -Lab
Total Hours: 60

L	T	P	Cr
0	0	4	2

Course Objectives:
The objective of this course is to provide students with hands-on experience in implementing advanced data structures and algorithms to solve complex computational problems efficiently. The course aims to strengthen students' understanding of algorithm design and analysis through practical experimentation with structures such as AVL trees, B-trees, heaps, graphs, and hashing techniques. By working through a range of coding exercises and real-world problem scenarios, students will develop proficiency in writing optimized, modular, and reusable code. This lab also fosters critical thinking and debugging skills necessary for high-performance software development.

Course Learning Outcomes:
After completion of course, students would be able to:
CLO1: Design and analyse different data structures·
CLO2: Identify the appropriate data structure for a given algorithm.
CLO3: Implement various data structures and algorithms.

Lab Assignments

As per the teaching Learning in the Theory Class

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

Component	**Marks**
Continuous Evaluation	60
End Term (Implementation and Viva-Voce)	40
Total	**100**

Suggested Readings:

1. Lab Manual
2. Allen Weiss M. (2014). Data Structures and Algorithm Analysis in C++. New Delhi: Pearson Education

Course Code: CBS.511
Course Title: Intrusion Detection System Lab
Total Hours: 30

L	T	P	Cr
0	0	2	1

Course Objectives:
The objective of this course is to familiarize students with the practical aspects of Intrusion Detection Systems (IDS), enabling them to simulate, implement, and analyze various IDS techniques and tools. The lab offers an experiential learning environment where students gain exposure to both signature-based and anomaly-based detection methods, and learn to work with real-world IDS platforms like Snort, Suricata, or Bro/Zeek. The course aims to develop students' skills in identifying potential security threats, configuring IDS rules, analysing alerts, and evaluating system performance to mitigate cyber-attacks effectively.

Course Learning Outcomes:
After completion of course, students would be able to**:**
CLO1: Apply knowledge of the fundamentals of Intrusion Detection in order to avoid common pitfalls in the creation and
CLO2: Implement new Intrusion Detection Systems.
CLO3: Evaluate Intrusion Detection tools and techniques in order to improve their security posture.

Lab Assignments
Practical will be based on as per the teaching Learning in the Theory Class

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

Component	**Marks**
Continuous Evaluation	60
End Term (Implementation and Viva-Voce)	40
Total	**100**

Suggested Readings:

1. Lab Manual
2. Szor, P. (2010). The Art of Computer Virus Research and Defense, United States: Symantec Press.

Course Code: CBS.509
Course Title: Python Programming for Cyber Security Lab
Total Hours: 30

L	T	P	Cr
0	0	2	1

Course Objectives:
The outcome of this lab course is to provide a practical introduction to python programming and its use in performing activities related to cyber security. Another objective of this lab is to demonstrate the use of various packages for cyber security.

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

CLO1: Create and demonstrate script in Python by using basic constructs and control statements of Python.
CLO2: Illustrate the use of OOPS and file handling concept for data handling and visualisation.
CLO3: Develop python scripts to perform various activities related to ethical hacking.
CLO4: Develop python scripts to perform various activities related to cyber forensics.

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

Lab Assignments

Practical will be based on as per the Teaching Learning in the Theory Class**.**

Lab Evaluation:

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

Component	**Marks**
Continuous Evaluation	60
End Term (Implementation and Viva-Voce)	40
Total	**100**

Suggested Readings:

1. Lab Manual

Course Code: CBS.610
Course Title: Cryptography Lab
Total Hours: 30

L	T	P	Cr
0	0	2	1

Course Objectives:

The objective of this course is to introduce students to the foundational concepts of security, including the various types of attacks that can compromise system integrity. It aims to provide a thorough understanding of both Symmetric and Asymmetric Key Cryptography techniques, enabling students to grasp their mechanisms, applications, and significance in securing communication. Additionally, the course discusses key application layer protocols, helping students comprehend their roles and vulnerabilities within a secure network architecture.

Course Learning Outcomes::
CLO1: Identify the domain specific security issues.
CLO2: Implement Symmetric & Asymmetric Key Cryptography algorithms.

Lab Assignments
Practical will be based on as per the Teaching Learning in the Theory Class**.**

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

Component	**Marks**
Continuous Evaluation	60
End Term (Implementation and Viva-Voce)	40
Total	**100**

Suggested Readings:

1. Lab Manual
2. Forouzan, B. A. (2010). Cryptography & Network Security. New Delhi: Tata McGraw-Hill Education.
3. Kahate, A. (2009). Cryptography and Network Security. New Delhi: tata McGraw-Hill Higher E

Course Code: CBS.510
Course Title: Ethical Hacking Lab
Total Hours: 30

L	T	P	Cr
0	0	2	1

Course Objectives:

The objective of this course is to provide students with hands-on experience in ethical hacking tools and techniques used to identify and mitigate security vulnerabilities in computing systems. It aims to enhance students' understanding of network, web, and system-level threats by allowing them to practically apply ethical hacking methodologies in controlled environments. The course fosters skill development in penetration testing, vulnerability assessment, and the use of various open-source and commercial tools, thereby preparing students to contribute effectively to organizational cybersecurity.

Course Learning Outcomes::

Upon successfully completing this course, students will be able to:
CLO1: Select appropriate tool for various activities related to ethical hacking
CLO2: Design an ethical hacking plan
CLO3: Identify various vulnerabilities
CLO4: Write test reports

Lab Assignments

Practical will be based on as per the Teaching Learning in the Theory Class**.**

Lab Evaluation:

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

Component	**Marks**
Continuous Evaluation	60
End Term (Implementation and Viva-Voce)	40
Total	**100**

Suggested Readings:

1. Lab Manual
2. Baloch, R. (2015). Ethical Hacking and Penetration Testing Guide. London: CRC Press.

Course Code: CBS. 611
Course Title: Linux OS and Scripting Lab
Total Hours: 30

L	T	P	Cr
0	0	2	1

Course Objectives: The Linux OS and Scripting Lab aims to provide students with hands-on exercises that reinforce their understanding and knowledge of various linux commands and scripting aspects.

Course Learning Outcomes:
CLO1: Demonstrate the use of various linux commands.
CLO2: Implement various scripts.

Lab Assignments
Practical will be based on as per the Teaching Learning in the Theory Class**.**

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

Component	**Marks**
Continuous Evaluation	60
End Term (Implementation and Viva-Voce)	40
Total	**100**

Suggested Readings:

1. Lab Manual

Course Code: CBS.516
Course Title: Information Theory Lab
Total Hours: 30

L	T	P	Cr
0	0	2	1

Course Objectives:
The objective of this course is to provide deeper knowledge about information theory and entropy concepts, enabling students to understand the fundamental principles of data representation and transmission. It aims to deliver an in-depth understanding of various coding techniques such as block codes, cyclic codes, and parity check codes, which are essential in error detection and correction. The course also focuses on developing practical skills through hands-on experience with both lossless and lossy compression techniques. Furthermore, it equips students with the knowledge required to apply advanced compression methods in real-world scenarios.

Course Learning Outcomes:

After completion of course, students would be able to:

CLO1: Determine the various entropies and mutual information for different channels.
CLO2: Construct the codes to secure the information during communication using different coding techniques.
CLO3: Implement and analyse the source coding and channel coding for transmitting the different objects like text, speech etc.
CLO4: Analyse the performance of coded and un-coded communication systems based on error probability.
CLO5: Implement and analyse different compression techniques for different objects like Image, Video and Audio etc.

Lab Assignments
Practical will be based on as per the Teaching Learning in the Theory Class**.**

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

Component	**Marks**
Continuous Evaluation	60
End Term (Implementation and Viva-Voce)	40
Total	**100**

Suggested Readings:
1. Lab Manual

Course Code: CBS.517
Course Title: Number Theory Lab
Total Hours: 30

L	T	P	Cr
0	0	2	1

Course Objectives:
The objective of this course is to provide a deeper understanding of the principles and practical applications of number theoretic algorithms. It aims to help students identify how number theory forms the foundation for designing cryptographic algorithms. Additionally, the course offers both theoretical knowledge and hands-on experience, enabling students to apply number theoretic algorithms and theorems to solve research problems across various fields.

Course Learning Outcomes:

At the end of the course the student will be able to:

CLO1: Implement and analyse the Number Theoretic algorithms.
CLO2: Implement the Fermat's theorem, Euler's theorem and Chinese reminder theorem to solve Congruences equations appear in different research problem.
CLO3: Implement and analyse the Primality test and factorization algorithms to understand the various cryptosystems.
CLO4: How to use Number Theoretic concepts in various research problems of Computer Science and in other fields.

Lab Assignments
Practical will be based on as per the Teaching Learning in the Theory Class**.**

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

Component	**Marks**
Continuous Evaluation	60
End Term (Implementation and Viva-Voce)	40
Total	**100**

Suggested Readings:
1. Lab Manual

Interdisciplinary Course (IDC) Semester-I

Course Code: CBS.518
Course Title: IT Fundamentals
Total Hours: 30

L	T	P	Cr
2	0	0	2

Course Objectives:

The course aims to provide a comprehensive understanding of the foundational concepts in Information Technology. It introduces students to essential topics such as computer hardware, software, networking, data storage, operating systems, and the internet. The course also emphasizes practical applications, enabling students to effectively use IT tools for academic and professional tasks. By the end of the course, students will develop the confidence to analyze, interpret, and engage with various IT systems and appreciate the role of IT in solving real-world problems.

Course Learning Outcomes:

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

CLO1: Describe different hardware and software components of computer.

CLO2: Use word processing, presentation and spreadsheet software.

CLO3: Illustrate the concept of networking and internet.

Units/Hours	Contents	Mapping with Course Learning Outcome
I **8 Hours**	**Fundamentals of Computers:** Parts of computers, Hardware, BIOS, Operating systems, Binary system, Logic gates and Boolean Algebra. Introduction to computer network and World Wide Web, Storage space, CPU and Memory.	**CLO1**
	Activities: Numerical Based exercises for conversion of Binary to octal, hexadecimal and decimal number system, Identification of various ports by the students on such as Audio ports, USB ports, HDMI Port, Ethernet port	
II **7 Hours**	**MS-Word:** Introduction to Word Processing, Creating and Saving Documents, Text Formatting, Tables, Document Review Option, Mail Merge, Inserting Table of Contents, Reference Management.	**CLO2**
	Activities: Error free typing exercises, Insertion of in text citations and insertion of Bibliography at the end of the document, Insertion of Tables and figures and cross referencing them from the text.	

III **8 Hours**	**Applications Software:** Introduction to MS Paint, Notepad, Spreadsheet applications, Presentation applications, Internet browsers and Image processing applications.	**CLO2**
	Activities: Creation of a Powerpoint presentation by students with various animation and and transition effects, Creation of an excel workbook by the students and application of basic mathematical functions (such as sum, average, Count, Mean, Median, Mode) on the data	
IV **7 Hours**	**World Wide Web:** Origin and concepts, Latency and bandwidth, searching the internet, Advanced web-search using Boolean logic, Networking fundamentals.	**CLO3**
	Activities: searching for some relevant articles using keyword combinations on various electronic databases using advanced search options by students.	

Transactional Modes:

- Lecture
- Blended Learning
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Gookin, D. (2007). MS Word for Dummies. United States: Wiley.
2. Harvey, G. (2007). MS Excel for Dummies. United States: Wiley
3. Sinha, P.K. (2004). Computer Fundamentals. New Delhi: BPB Publications.
4. Bott, E. (2009). Windows 7 Inside Out. United States: Microsoft Press.
5. Goel, A., Ray, S. K. (2012). Computers: Basics and Applications. New Delhi: Pearson Education India.
6. Research Articles from SCI & Scopus indexed Journals.

Course Code: CBS.519
Course Title: Programming in C
Total Hours: 30

L	T	P	Cr
2	0	0	2

Course Objectives:

This course is designed to develop a strong foundation in programming using the C language, which is critical for understanding system-level and application-level software development. The objective is to enable students to write structured, efficient, and error-free programs by understanding fundamental programming constructs such as variables, control structures, functions, arrays, pointers, and file handling. Students will also gain insight into memory management and algorithmic thinking, preparing them to handle more complex programming tasks and transition smoothly into other advanced languages and systems programming.

Course Learning Outcomes:

At the end of this course, students will be able to:
CLO1: Describe the concept and need of programming.
CLO2: Explain syntax and use of different functions available in C.
CLO3: Demonstrate programming in C.

Units/Hours	**Contents**	**Mapping with Course Learning Outcome**
I **8 Hours**	**Introduction to Programming Language:** Types of Programming Language, Structured Programming, Algorithms and Flowcharts, Programming Language. **Introduction to C:** History, Character Set, Structure of a C Program – constants, variables and Keywords, data types, expression statements, compound statements.	**CLO1** **CLO2**
	Activities: Program Fragments based exercises to find out output of various program fragments using the studied concepts	
II **8 Hours**	**C Operators:** Arithmetic, Unary, Relational and Logical, Assignment, Conditional Operator, Increment, decrement Operator, Using library function in math. **Data Input Output:** Single character input, getchar, getch, getc, single character output putchar, putc, Formatted I/O.	**CLO2,** **CLO3**
	Activities: Program Fragments based exercises.	
III **7 Hours**	**C Constructs:** If statement, while statement, do….while statement, for statement, switch statement, nested control statement, break, continue, goto statement. **C Functions:** Functions, Definition and scope, Assessing and Prototyping, Types of functions, passing arguments to functions.	**CLO2,** **CLO3**

	Activities: Program fragments-based exercises, Creating User defined function to perform simple activities and using them in C program.	
IV **7 Hours**	**Arrays and Strings:** Single dimensional array, Multi-dimensional array, initializing array using static declaration, character array and strings, String Handling functions.	**CLO2, CLO3**
	Activities: Program fragment-based exercises, Pseudocode to implement single and multi-dimensional arrays concept for practical programs.	

Transactional Modes:

- Lecture
- Blended Learning
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Rajaraman, V. (2008). Computer Basics and C Programming PHI Learning.
2. Brown, T. D. (1987) C for Basic Programmers. United States: Silicon Press.
3. Kanetkar, Y. P. (2010). Let Us C. New Delhi: BPB Publications.
4. Balagurusamy. (2008). Programming in ANSI C. New Delhi: Tata Mcgraw-Hill.
5. Research Articles from SCI & Scopus indexed Journals.

Course Code: CST.530
Course Title: Introduction to Digital Logic
Total Hours: 30

L	T	P	Cr
2	0	0	2

Course Objectives:

The course introduces the principles of digital logic design and its application in the development of digital systems. It covers topics such as number systems, logic gates, Boolean algebra, combinational and sequential circuits, and memory elements. The objective is to help students understand how digital circuits work at the logic level and how they form the basis of computer architecture. By the end of the course, students will be equipped with the skills to design and analyze digital systems, laying the groundwork for further study in embedded systems, computer architecture, and hardware design.

Course Learning Outcomes:

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

CLO1: Describe the digital signal along with the operations applicable on them.

CLO2: Discuss different number systems and conversion between them along with memory devices used to store such data.

CLO3: Apply the Boolean laws in different situation.

Units/Hours	Contents	Mapping with Course Learning Outcome
I 8 Hours	**Introduction:** Digital Signals, basic digital circuits: AND operation, OR operation and NOT operation. **Number Systems:** Introduction, Binary number system, Octal number system, Hexadecimal Number system, Conversion of one number system to other, Gray code.	CLO-1
	Activities: Web based Simulation learning.	
II 8 Hours	**Logic Gates and Boolean Algebra**: Boolean Laws, Boolean expression and functions, Logic Gates.	CLO-2
	Activities: Web based Simulation learning.	
III 7 Hours	**Combinational Circuit Design:** Karnaugh Map representation of logic functions, SOP, POS, Simplification of logic functions using K-Map.	CLO-2
	Activities: Exercise based learning.	
IV 7 Hours	**Flip-Flops:** 1-bit memory cell, S-R Flip Flop, J-K Flip Flop, D-Flip Flop, T- Flip Flop.	CLO-2
	Activities: Web based simulation.	

Transactional Modes:

- Lecture
- Blended Learning
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Mano, M. and Charles, K. (2007). Logic and Computer Design Fundamentals. New Delhi: Pearson Education.
2. Jain, R.P. (2006). Modern Digital Electronics. New Delhi: Tata McGraw Hill.
3. Kharate, G.K. (2010). Digital Electronics. United States: Oxford Higher Education.
4. Research Articles from SCI & Scopus indexed Journals.

Course Code: CST.531
Course Title: Multimedia and Its Applications
Total Hours: 30

L	T	P	Cr
2	0	0	2

Course Objectives:

This course provides an overview of multimedia technologies and their applications in various domains such as education, entertainment, communication, and digital content creation. The objective is to familiarize students with multimedia components including text, graphics, audio, video, and animation, as well as multimedia systems, formats, and tools. Students will explore how multimedia is stored, processed, compressed, and transmitted across platforms. The course also emphasizes hands-on experience with multimedia software to encourage creative expression and practical problem-solving.

Course Learning Outcomes:

At the end of this course, students will be able to:
CLO1: Identify and analyze different types of multimedia along with their representation.
CLO2: Differentiate between formats of all types of multimedia.
CLO3: Plan where we can use this multimedia.

Units/Hours	Contents	Mapping with Course Learning Outcome
I **8 Hours**	**Introductory Concepts:** Multimedia-Definitions, Basic properties and medium types. Multimedia applications, Uses of Multimedia. **Sound/ Audio:** Basic Sound Concepts, Music. **Speech:** Generation, Analysis and Transmission.	**CLO 1**
	Activities: Group Discussion.	
II **7 Hours**	**Images and Graphics:** Basic concepts: Image representation, image format, Graphics Format, Computer Image Processing. **Video and Animation:** Basic Concepts: Video Signal Representation, Computer Video Format. Television: Conventional Systems, Enhanced Definition Systems, High-Definition Systems.	**CLO 2**
	Activities: Web based learning.	
III **7 Hours**	**Data Compression:** Storage space, coding requirements, JPEG, MPEG. **Miscellaneous:** Optical Storage Media, Mutlimedia Operating Systems, Multimedia Communication Systems.	**CLO 3**
	Activities: Simulation based Learning.	

IV **8 Hours**	**Documents and Hypertext:** Document Architecture, Manipulation of Multimedia Data, Hypertext, Hypermedia and Multimedia and example. **Multimedia Applications:** Media Preparation, composition, Integration, communication, Consumption, and Entertainment.	**CLO 3**
	Activities: Group Discussion.	

Transactional Modes:

- Lecture
- Blended Learning
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Steinmetz, R. (2009). Multimedia: Computing Communications & Applications. New Delhi: Pearson Education India.
2. Vaughan, T. (2008). Multimedia: making it work. New Delhi: Tata McGraw-Hill Education.
3. Rao, K.R., Bojkovic, Z. S. and Milovanovic, D. A. (2002). Multimedia Communication Systems: Techniques, Standards, and Networks. United States: Prentice Hall.
4. Andleigh, P.K. (2007). Multimedia Systems Design. United States: Prentice Hall
5. Rimmer, S. (2007). Advanced Multimedia Programming. New Delhi: Windcrest/McGraw-Hill.
6. Research Articles from SCI & Scopus indexed Journals.

Course Code: CST.532
Course Title: Introduction to MATLAB
Total Hours: 30

L	T	P	Cr
2	0	0	2

Course Objectives:
The course aims to introduce MATLAB as a powerful computational and visualization tool for engineering and scientific applications. Students will learn the basics of MATLAB programming, including matrix operations, control structures, data visualization, and function creation. The objective is to enable students to solve mathematical problems, analyze data, and simulate systems using MATLAB's built-in functions and toolboxes. This foundation will support further exploration of signal processing, machine learning, and numerical computation in advanced courses and research work.

Course Learning Outcomes:
At the end of this course, students will be able to:
CLO1: Describe the basic syntax of MATLAB along with various functions available in it.
CLO2: Analyze all the functions in graphical manner.
CLO3: Design a GUI interface for any software.

Units/Hours	Contents	Mapping with Course Learning Outcome
I **8 Hours**	**Introduction**: MatLab, MatLab Syntax and interactive computations. Live Demonstration of MATLAB command prompt.	**CLO 1**
	Activities: Assignment based learning.	
II **7 Hours**	**Programming:** in Matlab using procedures and functions: Arguments and return values, M-files, Formatted console input-output, String handling. Live Demonstration of MATLAB M-files	**CLO 1,** **CLO 2**
	Activities: Assignment based learning	
III **8 Hours**	**Control Statements:** Conditional statements: If, Else, Elseif. Repetition statements: While, For. **Manipulating Text:** Writing to a text file, Reading from a text.	**CLO 2**
	Activities: Creation of text files and assignment-based learning.	
IV **7 Hours**	**Graph Plots:** Basic plotting, Built in functions **GUI Interface:** Attaching buttons to actions, Getting Input, Setting Output Using the toolboxes.	**CLO 3**

Transactional Modes:

- Lecture
- Blended Learning
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Attaway. (2012). Matlab: A Practical Introduction to Programming and Problem Solving. Elsevier
2. Pratap, R. (2010). Getting Started with MATLAB: A Quick Introduction for Scientists and Engineers. New Delhi: Oxford.
3. Research Articles from SCI & Scopus indexed Journals.

Course Code: CST.607
Course Title: Basics of Python Programming
Total Hours: 32

L	T	P	Cr
2	0	0	2

Course Objectives:

The objective of this course is to introduce students to the foundational concepts of programming using Python. It aims to develop an understanding of programming logic, control structures, and core Python constructs such as variables, operators, lists, dictionaries, and functions. The course also focuses on practical skills such as file handling, working with structured data formats (CSV, Excel, PDF, Word), and data visualization using libraries like pandas and matplotlib. Through hands-on lab sessions, students will gain the ability to write, debug, and implement Python programs for real-world problem-solving and data analysis tasks.

Course Learning Outcomes

After the completion of course, participants will be able to:

CLO1: Explain basics of programming.

CLO2: Define various constructs of python programming.

CLO3: Develop python code to handle data stored in files.

CLO4: Develop python code to represent the data in graphical mode.

Units/Hours	**Contents**	**Mapping with Course Learning Outcome**
I **8 Hours**	Introduction to algorithm, flowchart and programming, Python Introduction, Installing and setting Python environment, variables and its types, Operators. Flow control: if, if-else, for, while, range () function, continue statement, pass statement.	**CLO-1**
	Activities: Lab based practices for above concepts.	
II **8 Hours**	Lists: Basic Operations, Iteration, Indexing, Slicing. Dictionaries: Basic dictionary operations, Basic String operations.	**CLO-2,** **CLO-4**
	Activities: Lab based practices for above concepts.	
III **8 Hours**	Functions: Definition, Call, Arguments. Pattern Matching with Regular Expressions, Introduction to panda's library, plotting data using matplotlible.	**CLO-3**
	Activities: Lab based practices for above concepts.	**CLO-4**
IV **8 Hours**	File handling: Reading and Writing Files, working with Excel Spreadsheets, working with PDF and Word Documents, working with CSV Files.	
	Activities: Lab based practices for above concepts**.**	

Transactional Modes:

- Lecture
- Blended Learning
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Sweigart, AI. (2014). Automate the Boring Stuff with Python Practical Programming for Total Beginners. Switzerland: No Starch Press.
2. Mark, L. (2013). Learning Python. California: Oreilly Media.
3. Research Articles from SCI & Scopus indexed Journals.

SEMESTER –II

Course Code: CST. 508
Course Title: Machine Learning
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:
To help students explain the concept of how to learn patterns and concepts from data without being explicitly programmed. To analyze various machine learning algorithms and techniques with a modern outlook focusing on recent advances.

Course Learning Outcomes:
After completion of course, students would be able to:
CLO1: Describe machine learning approaches.
CLO2: Discuss features that can be used for a particular machine learning approach in various applications.
CLO3: Compare and contrast pros and cons of various machine learning techniques.
CLO4: To mathematically analyze various machine learning approaches and paradigms.
CLO5: Formulate various machine learning and ensemble methods for use in IOT applications.

Units/Hours	**Contents**	**Mapping with Course Learning Outcome**
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	**CLO1**
	Activities: Brainstorming, assignment-based learning.	
II **14 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)	**CLO1** **CLO 2**
	Activities: Exercise based learning and practical hands on training	
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.	**CLO2** **CLO4**

	Introduction to ANN and Deep learning. **Activities:** Exercise based learning and practical hands on training	
IV **16 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. **Activities:** Analysis of various case studies.	**CLO2** **CLO5**

Transactional Modes:

- Lecture cum Demonstration
- Collaborative Learning
- Peer Learning/Teaching
- Experimentation
- Online Teaching Tools

Suggested Readings:

1. Murphy, K. (2012). Machine Learning: A Probabilistic Perspective. Cambridge: MIT Press.
2. Hastie, T., Tibshirani, R., and Friedman, J. (2009). The Elements of Statistical Learning. New York: Springer.
3. Bishop, C. (2007). Pattern Recognition and Machine Learning, New York: Springer.
4. Shalev-Shwartz, S., and Ben-David, S. (2014). Understanding Machine Learning: From Theory to Algorithms. New Delhi: Cambridge University Press.

Course Code: CST.540
Course Title: Multimedia Security
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:

Provide a framework to conduct research and development using multimedia security techniques. Impart the knowledge of implementation on digital watermarking and multimedia security techniques. Design a customary multimedia security system to suit real world applications.

Course Learning Outcomes:

After completion of course, students would be able to:

CLO1: Learn the basic watermarking techniques to design a good digital mark.

CLO2: Study the digital authentication and authorization schemes to evaluate security issues related to electronic documents, images and video.

CLO3: Analyze the basic characteristics of digital watermarking to perform the theoretical analysis and performance measures.

CLO4: Acquire the concepts of steganography to access the sensitive information concealing of file, message, image, or video within another file.

CLO5: Examine the multimedia encryption techniques to address the open issues related to the confidentiality of the media content.

Units/Hours	Contents	Mapping with Course Learning Outcome
I **16 Hours**	Digital Watermarking: Introduction, History, Classification (Characteristics and Applications), Types and Techniques (Spatial-domain, Frequency-domain, and Vector quantization-based watermarking), Watermark security & authentication. Watermarking techniques: non-cryptographic and cryptographic; encoding and decoding; partial encryption	**CLO-1** **CLO-2**
	Activities: Lab based practices for above concepts. Simulation based Learning.	
II **16 Hours**	Media-Specific Digital Watermarking: Image watermarking, video watermarking, audio watermarking, Watermarking for Streaming Media, Forensic Watermarking, Robustness to Temporal and Geometric Distortions, Affine resistant transformation. Attacks and Tools (Attacks by Filtering, Remodulation, Distortion, Geometric Compression, Linear Compression etc.),	**CLO-1** **CLO-2**
	Activities: Lab based practices for above concepts. Assignment based learning	

III **16 Hours**	Steganography: Overview, History, Modern Steganography, Steganography Channels, Steganography Goals Methods for hiding (text, images, audio, video, speech etc.), Issues: Security, Capacity and Imperceptibility, Difference between Watermarking and Steganography. Steganography in Social Media Platforms Steganalysis: Active and Malicious Attackers, Active and passive steganalysis.	**CLO-3**
	Activities: Lab based practices for above concepts.	
IV **16 Hours**	Frameworks for secret communication (Pure Steganography, Secret key, Public key steganography), Steganography techniques: Substitution systems, Spatial Domain, transform domain techniques, Spread spectrum, Statistical steganography Detection, Distortion, Techniques, Multimedia Security Threats, Multimedia Threat Intelligence, Multimedia-based Ransomware Attacks, Multimedia Data forgeries – Techniques, detection and prevention mechanisms, Multimedia Encryption.	**CLO-2** **CLO-3**
	Activities: Lab based practices for above concepts.	

Transactional Modes:

- Lecture
- Blended Learning
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Cox, Miller, Bloom, Fridrich, Kalker (2007). Digital Watermarking and Steganography: Morgan Kaufmann.
2. Borko Furht and Darko Kirovski (2020). Multimedia Security Handbook: CRC Press.
3. Borko Furht and Darko Kirovski (2019). Multimedia Watermarking Techniques and Applications: CRC Press
4. Sencar HT, Verdoliva L, Memon N. (2022). Multimedia Forensics: Springer.
5. Chang-Tsun Li (2008). Multimedia Forensics and Security: IGI Global.
6. Aboul Ella Hassanien, Mohamed Mostafa Fouad, Azizah Abdul Manaf, Mazdak Zamani (2017). Multimedia Forensics and Security: Foundations, Innovations, and Applications: Academic Press.
7. K. J. Ray Liu, Wade Trappe, Z. Jane Wang (2005). Multimedia Fingerprinting Forensics for Traitor Tracing: Hindawi Publishing Corporation.

Course Code: CBS.521
Course Title: Malware Analysis & Reverse Engineering
Total Hours: 60

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.

Course Learning Outcomes:

After completion of course, students would be able to:
CLO1: Understand the concept of malware and reverse engineering.
CLO2: Implement tools and techniques of malware analysis.
CLO3: Applying debugging concept with tools
CLO4: Learning Memory Forensic and Volatility

Units/Hours	Contents	Mapping with Course Learning Outcome
I **15 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.	**CLO-1**
	Activities : Use of Sandbox to understand the Malware	
II **14 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	**CLO-2**

	Packers using PEiD, Registry Forensics with Reg Ripper Plugins:, Bypassing Poison Ivy's Locked Files, Bypassing Conficker's File System ACL Restrictions, Detecting Rogue PKI Certificates.	
	Activities: Use of web-based tools to understand the concepts.	
III **14 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.	**CLO-3**
	Activities: Use of Python Libraries to understand the concepts.	
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.	**CLO-4**
	Activities: Case study of Finding Artifacts in Process Memory, Identifying Injected Code with Malfind and YARA.	

Transactional Modes:

- Lecture cum Demonstration
- Peer Learning/Teaching
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Sikorski, M. & Honig, A. (2012). Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. San Francisco: publisher William Pollock No Starch Press.
2. Ligh, M. H., Case, A., Levy, J., & Walters, A. (2014). The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. United States: Wiley.
3. Research Articles from SCI & Scopus indexed Journal

Course Code: CBS.523
Course Title: Secure Software Design and Enterprise Computing
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:

To help students learn 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.

Expose students to techniques for successfully implementing and supporting network services on an enterprise scale and heterogeneous systems environment.

Course Learning Outcomes:

After completion of course, students would be able to:
CLO1: Show Interrelationship between security and software development process.
CLO2: Differentiate between various software vulnerabilities.
CLO3: Explain software process vulnerabilities for an organization.
CLO4: Recognize resources consumption in a software.

Units/Hours	Contents	Mapping with Course Learning Outcome
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.	**CLO-1 and CLO-2**
	Activities : Case study based learning.	
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.	**CLO-1**
	Activities: Group Discussion based learning.	
III	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).	**CLO-3**

16 Hours	**Activities:** Group discussion based learning.	
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.	**CLO-4**
	Activities: Case study of various server configuration.	

Transactional Modes:

- Lecture cum Demonstration
- Peer Learning/Teaching
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Richardson, T., and Thies, C. N. (2012). Secure Software Design. Massachusetts: Jones & Bartlett Learning.
2. Kenneth R. van Wyk, Mark G. Graff, Dan S. Peters, and Diana L. Burley, (2014). Enterprise Software Security: A Confluence of Disciplines. United States: Addison - Wesley, Professional.
3. McGraw, G. (2006). Software Security: Building Security. New Delhi: Tata McGraw.
4. Stuttard, D. (2011). The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. United States: Wiley.
5. Solem, J. E. (2012). Programming Computer Vision with Python: Tools and algorithms for analysing images. California: O'Reilly Media.
6. Research Articles from SCI & Scopus indexed Journal

L	T	P	Cr
4	0	0	4

Course Code: CBS.524
Course Title: Big Data Analytics and Visualization
Total Hours: 60
Course Objectives:

The course will help students prepare the big data for analysis and extract the meaningful data from unstructured big data. Help student to develop data visualizations skill and to apply various tools for analysis of structured and unstructured big data.

Course Learning Outcomes:

After completion of course, students would be able to:

CLO1: Illustrate the identification of Big Data problem

CLO2: Learn the Behaviour and Visualisation of Data

CLO3: Differentiate structured data from unstructured data.

CLO4: Use Hadoop related tools such as JAQL, Spark, Pig and Hive for structured and unstructured Big Data analytics.

Units/Hours	Contents	Mapping with Course Learning Outcome
I 15 Hours	Big Data Introduction: What is big data, why big data, convergence of key trends, unstructured data, industry examples of big data and web analytics. **Big Data Technologies: Big Data Architecture in PySpark, Spark ecosystem overview, Spark SQL, MLlib, Spark Streaming, RDD vs DataFrame vs Dataset, PySpark setup** Data Gathering and Preparation: Data formats, parsing and transformation, Scalability and real-time issues.	CLO1
	Activities: Case study and Group Discussion.	
II 15 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.	CLO2, CLO-3
	Activities: Implementation above theory with Python code.	
III 15 Hours	NoSQL: Introduction to NoSQL, aggregate data models, key-value and document data models. **Vector Databases: Introduction to Vector databases, Embedding Fundamental, Working with FAISS, Vector Database Schema and Metadata.**	CLO-3
	Activities: Implementation and designing with Spark/Mongo DB.	

IV **15 Hours**	**Text preprocessing:** Loading and cleaning raw text files, Tokenization, stop words, stemming, lemmatization (NLTK, spaCy) **Big Data Text Analytics:** Understanding Text Analytics in Big Data, Predictive Analysis with Text, Document-Term Matrix with `scikit-learn`, Basic sentiment analysis, Topic modeling (LDA), TF-IDF scoring and vectorization.	**CLO-4**
	Activities: Implementation and usage of tools over the cloud.	

Transactional Modes:

- Lecture cum Demonstration
- Peer Learning/Teaching
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. EMC Education Services. (2015). Data Science and Big Data Analytics: Discovering, Analyzing, Visualizing and Presenting Data. United States: John Wiley & Sons.
2. Maheshwari, A. (2019). Data Analytics Make Accesible. California: Orilley Publications.
3. Croll, A., and Yoskovitz, B. (2013). Lean Analytics: Use Data to Build a Better Startup Faster. California: Oreilley Publications.
4. Research Articles from SCI & Scopus indexed Journals.

Course Code: CST.524
Course Title: Internet of Things
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:

The objective of this course is to introduce the students to the concepts of IoT, its networking and communication. The course focussed on use of IoT technology and its design constraints.

Course Learning Outcomes:

After completion of course, students would be able to:

CLO1: Describe IoT and its networking and communication aspects.

CLO2: Analyze the IoT Design Methodology

CLO3: Explain the concepts related to Industry 4.0 and security.

CLO4: Design IoT applications on different embedded platform.

Units/Hours	Contents	Mapping with Course Learning Outcome
Unit-1 **16Hours**	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.	**CLO1**
	Activities: Assignments and Group Discussion.	
Unit-2 **14Hours**	IoT Platforms Design Methodology: Introduction, IoT Design Methodology, Case Study on IoT System for Weather Monitoring. Case Studies Illustrating IoT Design: Home Automation, Environment, Agriculture.	**CLO2**
	Activities: Analysis of various case studies	
Unit-3 **14Hours**	Introduction: Sensing & actuation, Industry 4.0: Cyber Physical Systems and Next Generation Sensors, Cybersecurity in Industry 4.0, Basics of Industrial IoT: Industrial Processes, Industrial Sensing & Actuation, Security in IIoT, Data Handling and Analytics.	**CLO3**
	Activities: Group Discussion and Flip Learning.	

Unit-4 **16Hours**	Developing IoTs: Developing applications through IoT tools including Python/ Arduino/ Raspberry pi, developing sensor-based application through embedded system platform.	**CLO4**
	Activities: Hands on experience with IoT kits.	

Transactional Modes:

- Lecture cum Demonstration
- Peer Learning/Teaching
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Sharma, S. (2018). *Smart Cities Unbundled*. Bloomsbury Publishing.
2. Kamal, R. (2017). *Internet of Things: Architecture and Design Principles*.
3. Chaudhuri, A. (2018). *Internet of Things, for Things, and by Things*. CRC Press.
4. Dargie, W., and Poellabauer, C. (2010). Fundamentals of Wireless Sensor Networks: Theory and Practice. Wiley-Blackwel.
5. DaCosta, F., and Henderson B. (2014). Rethinking the Internet of Things: A Scalable Approach to Connecting Everything, New York: Apress Publications.
6. Holler, J., Tsiatsis V., Mulligan, C., Avesand, S., Karnouskos, S., & Boyle, D. (2014). From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence. Massachusetts: Academic Press.

Course Code: **CBS 621**
Course Title: Web development and penetration testing
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:

This course focuses on providing students with a thorough grasp of web development principles and security practices. Through the course, students will acquire the ability to employ suitable tools and techniques for penetration testing web applications, effectively identify and address common web vulnerabilities, and evaluate the security status of web applications**.**

Course Learning Outcomes:

After completion of course, students would be able to:

CLO1: Develop a comprehensive understanding of web development concepts, techniques, and security measures.

CLO2: Apply appropriate tools and methodologies for penetration testing web applications.

CLO3: Demonstrate practical skills in identifying and mitigating common web vulnerabilities.

CLO4: Analyze and assess the security posture of web applications.

Units/Hours	**Contents**	**Mapping with Course Learning Outcome**
I **14 Hours**	Introduction to WebApplications, Architecture of web applications, Hyper Text Transfer Protocol Secure (HTTP), Hyper Text Transfer Protocol Secure (HTTPS). Front end Development using HTML: Creating Forms and Controls. Clientside scripting language - JavaScript: Variables and Objects, Decision Making Statement, Loops, Arrays, Functions, Applying Validations at Client Side.	**CLO1**
	Activities: Brainstorming, assignment based learning	
II **16 Hours**	Server Side Scripting: Introductionm to PHP, Language Fundamentals, Decision Making Statement, Loops, Statements, Operators, functions, Arrays, String OPerations, Processing Forms via GET/POST, Web Application Development, Introduction to PHP Frameworks. Data Management: Introduction to MySQL & its Versions, Administration & Query Browser, Creating Databases &	**CLO1**

	Tables, Using keys, Types of Table in MySQL, Data Types, Deleting databases and tables, Inserting, Retrieving, Updating & Deleting data, User Accounts, Access Control & documentation. PHP interfacing with MySQL	
	Activities: Exercise based learning and practical hands on training	
III **15 Hours**	Introduction to Penetration Testing standards, Pre Requirement of Pentration Testing, Penetration Testing Methodology, Setting up Vulnerable Web Application Lab, OWASP top 10 Web Vulnerabilites.Profiling the Web Server, Introduction to burpsuite,Authentication bypass using burpsuite, Bypassing Client Side Validations, Web Crawlers and Directory Bruteforce.	**CLO2** **CLO3**
	Activities: Exercise based learning and practical hands on training	
IV **15 Hours**	Authentication and Session Management Flaws, Detecting various Injection based vulnerabilites. Cross Site Request Forgery(CSRF), Server Side REquest Forgery(SSRF), Cross Site Scripting (XSS), Introduction to BeeF and browser Hijack, Uploading web shell, Path traversal, Local File Inclusion (LFI) and Remote File Inclusion (RFI)	**CLO3** **CLO4**
	Activities: Exercise based learning and practical hands on training	

Transactional Modes:

- Lecture
- Case Studies
- Collaborative
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Khawaja, G. (2018). Practical Web Penetration Testing: Packt Publisher.
2. Gutierrez, G.N. and Ansari, J.A (2018). Web Penetration Testing with Kali Linux. Packt Publisher.
3. Nixon, R. (2021). Learning PHP, MySQL & JavaScript: A Step-by-Step Guide to Creating Dynamic Websites, O'reilly Publishers.

Course Code: CBS 623
Course Title: Network Security
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives: The course is structured to uncover and understand the current trends in computer networks through literature readings and to encourage a performance-oriented approach to analysing computer and communications networks. It also provides hands-on experience in securing networks.

Course Learning Outcomes:
After completion of course, students would be able to:
CLO1: Describe the basics of networking and VLANS.
CLO2: Explain IP addressing, routing and subnetting.
CLO3: Demonstrate the configuration of Cisco Routers, IPv4 Addresses and Routes, DHCP, and Connectivity with ping, traceroute and telent.
CLO4: Design the network with Access Control Lists, Network Address Translation and Firewalls.

Units/Hours	Contents	Mapping with Course Learning Outcome
Unit I **14Hours**	Networking Fundamentals: Perspectives on Networking, TCP/IP Networking Model, OSI Networking Model. Ethernet LANs and Switches: Building Ethernet LANs with Switches, Installing and operating Cisco LAN Switches, Configuring Ethernet Switching. Virtual LAN: introduction to VLAN, VLAN Links, VLAN Tagging, VLAN Trunk Protocol (VTP).	**CLO1**
	Activities: Brainstorming, assignment-based learning	
II **16Hours**	Fundamentals of IPv4 Addressing and Routing: Overview of Network layer Functions, IPv4 Addressing: Rules for IP Addresses, Class A, B, and C IP networks. IPv4 Routing, IPv4 Routing Protocols. IPv4 Addressing and Subnetting: Perspectives on IPv4 Subnetting.	**CLO2**
	Activities: Exercise based learning and practical hands-on training	
Unit III	Implementing IPv4: Operating Cisco Routers, Configuring IPv4 Addresses and Routes: IP Routing, Configuring Connected Routes, Configuring Static Routes. Configuring and Verifying Host Connectivity: Configuring Routers to	

16Hours	Support DHCP, Verifying Host IPv4 Settings, Testing Connectivity with ping, traceroute and telent.	**CLO3**
	Activities: Exercise based learning and practical hands-on training	
Unit IV **14Hours**	Firewalls: Firewall Basics, Types of Firewalls: Packet Filter, State-full Filter, Application Filter, Proxy Firewalls, Network Address Translation: Basic concepts and NAT Configuration. Access Control Lists: Ingress and Egress Filtering, Types of Access Control Lists, ACL types: standard and extended, ACL commands. Wireless Network Security. implementation of Denial of service (DoS) attacks, Distributed DoS (DDoS) attack and various types of DoS attacks.	**CLO4**
	Activities: Exercise based learning and practical hands on training	

Transactional Modes:

- Lecture
- Case Studies
- Collaborative
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Riggs, C., & Group, T. &. F. (2019). *Network Perimeter Security: Building Defense In-Depth*. Auerbach Publications.
2. 2. Northcutt S. 2005. Inside Network Perimeter Security, 2nd Ed., Pearson Education
3. Stallings, W. (2017). *Network Security Essentials: Applications and Standards*.
4. Daimi, K. (2018). Computer and Network Security Essentials. In *Springer eBooks*. https://doi.org/10.1007/978-3-319-58424-9
5. Ibe, O. C. (2017). *Fundamentals of Data Communication Networks*. John Wiley & Sons.
6. Forouzan,B.A, 2009, Data Communications and Networking, 4th Ed. Tata McGraw Hill Education.

Course Code: CBS.527
Course Title: Digital Forensics
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:

The course provides an in-depth study of the rapidly changing and fascinating field of computer forensics. Introduces the students to the technical expertise and the knowledge required to investigate, detect and prevent digital crimes.

Course Learning Outcomes:

After completion of course, students would be able to:
CLO1: Describe relevant legislation and codes of ethics.
CLO2: Explain computer forensics, digital detective and various processes, policies and procedures.
CLO3: Apply E-discovery, guidelines and standards, E-evidence, tools and environment.
CLO4: Analyse Email and web forensics and network forensics.

Units/Hours	**Contents**	**Mapping with Course Learning Outcome**
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.	**CLO1**
	Activities Analysis of Cyber Attacks and laws with case studies.	
II **15 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.	**CLO2**

	Activities: Preparation of various documents related to Cyber Crime Investigation.	
III **14 Hours**	Image Capturing, Authenticating Evidence, Hidden Data Extraction, Data Storage, File Systems, Recovery of deleted files, Cracking Passwords, Internet Crime Investigations, Web Attack Investigations.	**CLO3** **CLO4**
	Activities: Demonstration of various tools to perform digital forensics.	
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.	**CLO4**
	Activities: Analysis of Case Studies, Performing various activities to perform network and mobile forensics.	

Transactional Modes:

- Lecture
- Case Studies
- Collaborative
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Oettinger, W.(2022). Learn Computer Forensics Your one-stop guide to searching, analyzing, acquiring, and securing digital evidence, 2nd Edition, Packt Publisher.
2. Sammons, J. (2014). The Basics of Digital Forensics, Elsevier.
3. Davidoff, S., and Ham, J. (2012). Network Forensics Tracking Hackers through Cyberspace. United States: Prentice Hall.
4. Solomon, M. G., Rudolph, K., Tittel, E., Broom, N., and Barrett, D. (2011). Computer Forensics Jump Start. United States: Willey Publishing.
5. Marcella, A. J., Cyber forensics: A field manual for collecting, examining and preserving evidence of computer crimes. New York: Auerbach publications.
6. Davidoff, S. (2012). Network forensics: Tracking hackers through cyberspace. New Delhi: Pearson education India.
7. Godbole, Nina, Belapure, Sunit (2011). Cyber security: Understanding cybercrimes, computer forensics and legal perspectives. New Delhi: Wiley India.
8. Casey, Eoghan (Ed.). (2010). Handbook of digital forensics and investigation, Amsterdam, Academic Press.
9. Research Articles from SCI & Scopus indexed Journals.

L	T	P	Cr
4	0	0	4

Course Code: CBS.525
Course Title: Secure Coding
Total Hours: 60

Course Objectives:

The outcome of this course is to explain the most frequent programming errors leading to software vulnerabilities and identify security problems in software.

Course Learning Outcomes:

After completion of course, students would be able to:
CLO1: Define secure programs and list various risks in the software.
CLO2: Classify different errors that lead to vulnerabilities.
CLO3: Analyse various possible security attacks.

Units/Hours	Contents	Mapping with Course Learning Outcome
I **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.	**CLO-1**
	Activities: Group Discussion based learning.	
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 Secity: Integer data Type, Integer Conversions, Integer Operations, Integer Vulnerabilities, Mitigation Strategies.	**CLO-2**
	Activities: Implementation of above concepts in various programming Languages.	

III **14 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.	**CLO-3**
	Activities: Implementation of above concepts in various programming Languages.	
IV **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.	**CLO-3**
	Activities: Implementation of above concepts in various programming Languages.	

Transactional Modes:

- Lecture cum Demonstration
- Peer Learning/Teaching
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Seacord, R. C. (2013). Secure Coding in C and C++. United States: Addison Wisley Professional.
2. Chess, B., and West J. (2007). Secure Programming with static Analysis. United States: Addison Wisley.
3. Seacord, R. C. (2009). The CERT C Secure Coding Standard. Pearson Education, United Stated: Addison-Wesley.
4. Howard, M., LeBlanc, D. (2002). Writing Secure Code. New Delhi: Pearson Education.
5. Research Articles from SCI & Scopus indexed Journals.

Course Code: **CBS 622**
Course Title: Hardware Security
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:

This course will focus on the importance of addressing different security threats on modern hardware design, manufacturing, installation, and operating practices. In particular, the threats would be shown to be relevant at scales ranging from a single user to an entire nation's public infrastructure. Through theoretical analyses and relevant practical world case studies, the threats would demonstrate, and then state-of-the-art defense techniques would be described. The course would borrow concepts from diverse fields of study such as cryptography, hardware design, circuit testing, algorithms, and machine learning.

Course Learning Outcomes:

After completion of course, students would be able:

CLO1: Understand and optimize the process of implementing cryptographic algorithms on hardware

CLO2: Learn the different kinds of attacks that can be mounted against cryptographic algorithms

CLO3: Learn the process of building Physical Unclonable Functions and make them resilient to attacks

CLO4: Understand the different kinds of Trojans, their impact and learn the effective countermeasures for defending against the and Learn the different kinds of threats at the microarchitectural level and their corresponding countermeasures.

Units/Hours	**Contents**	**Mapping with Course Learning Outcome**
I **15 Hours**	Hardware Security Primitives: Algebra of Finite Fields, Mathematics of Cryptography, Fundamentals of Digital Systems, Application-Specific Integrated Circuits (ASIC), Field Programmable Gate Arrays (FPGA).Cryptography Implementation: Symmetric Cryptography- DES, AES; Asymmetric Cryptography-RSA, ECC; Cryptographic Hardware and their Implementation, Optimization of Cryptographic Hardware on FPGA, Physically Unclonable	**CLO1**

	Functions (PUFs), PUF Implementations, PUF Quality Evaluation, Design Techniques to Increase PUF Response Quality	
	Activities: Assignment based learning	
II **15 Hours**	Side-channel Attacks on Cryptographic Hardware: Overview; Fault attacks and countermeasures; Power attacks and countermeasures, Current-measurement based Side-channel Attacks (Attack on DES), Design Techniques to Prevent Side-channel Attacks, Improved Side-channel Attack Algorithms (Template Attack, etc.), Cache Attacks. Testability and Verification of Cryptographic Hardware: Fault-tolerance of Cryptographic Hardware, Fault Attacks, Verification of Finite-field Arithmetic Circuits	**CLO2**
	Activities: Exercise based learning and practical hands on training	
III **14 Hours**	Modern IC Design and Manufacturing Practices and Their Implications: Hardware Intellectual Property (IP) Piracy and IC Piracy, Design Techniques to Prevent IP and IC Piracy, Using PUFs to prevent Hardware Piracy, Model Building Attacks on PUFs (Case Study: SVM Modeling of Arbiter PUFs, Genetic Programming based Modeling of Ring Oscillator PUF)	**CLO3**
	Activities: Case Studies	
IV **16 Hours**	Hardware Trojans: Hardware Trojan Nomenclature and Operating Modes, Countermeasures Such as Design and Manufacturing Techniques to Prevent/Detect Hardware Trojans, Logic Testing and Side-channel Analysis based Techniques for Trojan Detection, Techniques to Increase Testing Sensitivity Infrastructure Security: Impact of Hardware Security Compromise on Public Infrastructure, Defense Techniques	**CLO3**
	Activities: Group discussion	

Transactional Modes:

- Lecture
- Case Studies
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Bhunia, S., & Tehranipoor, M. (2018). Hardware security: a hands-on learning approach. Morgan Kaufmann.
2. Ahmad-Reza Sadeghi and David Naccache (eds.): Towards Hardware-intrinsic Security: Theory and Practice, Springer.
3. Rangarajan, N., Patnaik, S., Knechtel, J., Rakheja, S., & Sinanoglu, O. (2021). Next Era in Hardware Security. Springer International Publishing.
4. Tehranipoor, M., Pundir, N., Vashistha, N., & Farahmandi, F. (2023). Hardware Security Primitives. Springer International Publishing AG.

Course Code: CST.529
Course Title: Blockchain Technology
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:
The objective of this course is to introduce students to the concept of Blockchain, crypto primitives, Bitcoin basics, distributed consensus, consensus in Bitcoin, permissioned Blockchain, hyper ledger fabric and various applications where Blockchain is used.

Course Learning Outcomes::
After completion of course, students would be able to:
CLO1: Describe the basic concept of Blockchain, Crypto Primitives, Bitcoin Basics
CLO2: Identify the area in which they can apply permission or permission less Blockchain.
CLO3: Apply Block chaining concept in various applications.

Units/Hours	Contents	Mapping with Course Learning Outcome
I **14 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	**CLO-1**
	Activities: Case studies based Learning, Group Discussion.	
II **14 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.	**CLO-1**

	Activities: Live Demonstration, Implementation Based Learning of hash functions, Group Discussions.	
III **15 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	**CLO-2**
	Activities: Group Discussion, Assignment Based Learning, Case studies	
IV **17 Hours**	Blockchain Components and Concepts: Actors in a Blockchain, Components in Blockchain design, Ledger in Blockchain. Hyperledger Fabric architecture and design: Ordering Services, Channels in Fabric, Fabric Peer and Client application and fabric certificate authority. Hyperledger Fabric: Architecture and Transaction Flow. Hyperledger Membership and Identity Management: Organization and Consortium Network, Membership Service Provide, Transaction Signing.	**CLO-3**
	Activities: Assignment Based Learning, Live Demonstration.	

Transactional Modes:

- Lecture cum Demonstration
- Peer Learning/Teaching
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Gaur, N., Desrosiers, L., Ramakrishna, V., Novotny, P., Baset, S., & O'Dowd A. (2018). Hands-On Blockchain with Hyperledger: Building decentralized applications with Hyperledger Fabric and Composer. United Kingdom: Packt Publishing Ltd. Packt.

2. Badr, B., Horrocks, R., and Xun(Brian), Wu. (2018). Blockchain By Example: A developer's guide to creating decentralized applications using Bitcoin, Ethereum, and Hyperledger. United Kingdom: Packt Publishing Ltd.
3. Dhillon, V., Metcalf D., and Hooper M. (2017). Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You.New York: Apress.
4. Mukhopadhyay M. (2018). Ethereum Smart Contract Development: Build blockchain-based decentralized applications using solidity. United States: Packt Publishing Ltd.
5. Research Articles from SCI & Scopus indexed Journals.

Course Code: CBS.530
Course Title: Quantum Computing & Cryptography
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:

To provide fundamental concepts of quantum information processing and cryptography, and take the discussion forward to potentials offered, technological bottlenecks and the way forward. To expose the participants to the state-of-the-art in quantum computing and cryptography with its possible impact on the society.

Course Learning Outcomes

CLO1: Participants will understand the basic concepts and terminologies in quantum information processing and quantum cryptography.

CLO2: To work in the field of quantum information processing and quantum cryptography, and to design efficient quantum algorithms to solve different computing problems.

CLO3: To understand the basic concepts Non-local Correlation and Entanglement.

CLO4: To design new or modify existing quantum cryptographic algorithms for secure key distribution and communications.

CLO5: To grasp the working principle of a quantum computer and understand the impact of noise in real world implementations.

CLO6: To understand the current scenario in Google, IBM, D-wave, IonQ etc.

Units/Hours	Contents	Mapping with Course Learning Outcome
I **16 Hours**	Basics of Quantum Information and Linear Algebra: Why Quantum Computing, Classical to quantum mechanics, Hilber space, Bases vectors and linear independence, Operators and matrices, Hermitian and Unitary operators, Measurements in quantum mechanics.	**CLO-1, CLO-6**
	Activities : Exercise based learning, Demonstration of above theory using Mathemetica/ MATLAB tools	

II **14 Hours**	Introduction to quantum information: Qubits and quantum gates, Quantum circuits, Quantum parallelism, Bloch sphere, Bell states, Density operators, Pure and Mixed states, Information and entropy, Von-Neumann entropy.	**CLO-1,** **CLO-2**
	Activities: Activities: Assignment based learning, Demonstration of above theory using Mathemetica/ MATLAB tools	
III **14 Hours**	Quantum Distance Measures, Trace distance, Fidelity, No-cloning Theorem, Einstein-Podolsky-Rosen paradox, Entanglement and Nonlocality: Quantum entanglement, bi-partite and multiqubit systems, Bell-type inequalities and nonlocality, entanglement classes and measures.	**CLO-3**
	Activities: Assignment based learning, Demonstration of Entanglement and Non-locality through animated videos.	
IV **16 Hours**	Applications and Quantum Cryptography: Teleportation, Dense coding, Entanglement swapping, Quantum key distribution, Quantum cryptographic protocols (BB84, E91, BBM92), Quantum Random Number Generator, Introduction to Quantum Internets. Quantum Noise and Operation: Environments and quantum operations, examples of noisy channels, effect of noise on efficiency of communication protocols.	**CL0-4,** **CLO-5**
	Activities: Demonstration of above theory using Mathemetica/ MATLAB tools, Case based study of realization of quantum computing.	

Transactional Modes:

- Lecture cum Demonstration
- Peer Learning/Teaching
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Nielsen, M. A. and Chuang, I. L., (2010), Quantum Computation and Quantum Information, 10th Anniversary addition, Cambridge University Press
2. Griffiths, D. J., (2016), Introduction to Quantum Mechanics, Reprint edition, Pearson Prentice Hall, 2006.
3. Bouwmeester, D., Ekert, A. and Zeilinger, A., (2000), The Physics of Quantum Information, Reprint edition, Springer Berlin Heidelberg.

4. Quantum Computing A developers guide, Pierpaolo Marturano (2023) De Gruyter denbourg
5. Dancing with Python Learn to code with Python and Quantum Computing, Robert S. Sutor (2021) PacktPub
6. Introduction to Quantum Computing, Ray LaPierre (2021) Springer
7. Research Articles
8. Research Articles from SCI & Scopus indexed Journa

Course Code: CBS. 624
Course Title: Multimedia Security-Lab
Total Hours: 30

L	T	P	Cr
0	0	2	1

Course Objectives:

The objectives of the Multimedia Security-Lab course are to introduce students to the basic concepts and techniques of Image, Audio and Video Security. To develop skills using recent Computer Vision software for solving practical problems.

Course Learning Outcomes:

At the end of the course the student will be able to:

CLO1: Implement and analyse the Steganography techniques.
CLO2: Analyse and design of data hiding algorithms, like data embedding into multimedia objects.
CLO3: Implement different Water-Marking techniques and analyse Watermark security & authentication
CLO4: Analyse and Design of more robust Steganography and Water-Marking techniques against Malicious Attacks.
CLO5: Apply data hiding techniques in digital right management.
Students will implement the lab practical as per the syllabus of the subject.

Lab Assignment

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

Lab Evaluation:

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

Component	**Marks**
Continuous Evaluation	60
End Term (Implementation and Viva-Voce)	40
Total	**100**

Suggested Readings

1. Lab Manual

Course Code: CBS. 625
Course Title: Network Security Lab
Total Hours: 30

L	T	P	Cr
0	0	2	1

Course Objectives:

The Network Security Lab aims to provide students with hands-on exercises that reinforce their understanding and knowledge of various network security aspects.

Course Learning Outcomes:

CLO1: Demonstrate the configuration of VLANs, IP addressing, routing and subnetting.
CLO2: Implement IPv4 Addresses, Routes, DHCP and connectivity with ping, traceroute and telent.
CLO3: Design Access Control Lists and Network Address Translation

Lab Assignments

Practical will be based on as per the Teaching Learning in the Theory Class.

.

Lab Evaluation:

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

Component	**Marks**
Continuous Evaluation	60
End Term (Implementation and Viva-Voce)	40
Total	**100**

Suggested Readings:

1. Lab Manual

Course Code: CBS.531
Course Title: Malware Analysis & Reverse Engineering Lab
Total Hours: 30

L	T	P	Cr
0	0	2	1

Course Objectives:
The primary objective of this lab course is to provide a practical introduction to various techniques used for malware analysis and reverse engineering.

Course Learning Outcomes:

After completion of course, students would be able:

CLO1: to setup platform for malware analysis
CLO2: to use various tools available for malware analysis
CLO3: to analyse malware using reverse engineering.

Lab Assignments
Practical will be based on as per the Teaching Learning in the Theory Class**.**

Lab Evaluation:

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

Component	**Marks**
Continuous Evaluation	60
End Term (Implementation and Viva-Voce)	40
Total	**100**

Suggested Readings:

1. Lab Manual
2. Ligh, M. H., Case, A., Levy, J., & Walters, A. (2014). The Art of Memory Forensics: Detecting Malware and Threats in Wi

Course Code: CBS.533
Course Title: Secure Software Design & Enterprise Computing Lab
Total Hours: 30

L	T	P	Cr
0	0	2	1

Course Objectives:

To fix software flaws and bugs in various software. Students will aware of various issues like weak random number generation, information leakage, poor usability, and weak or no encryption on data traffic. Learn Methodologies and tools for developing secure software with minimum vulnerabilities and flaws.

Course Learning Outcomes:

After completion of course, students would be able to:
CLO1: Learn the use of various tools for software vulnerability.
CLO2: Apply different techniques for identification of software flaws.
CLO3: Track the resolution of flaws in software.
CLO4: Interrelate security and software development process.

Lab Assignments

Practical will be based on as per the Teaching Learning in the Theory Class**.**

Lab Evaluation:

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

Component	**Marks**
Continuous Evaluation	60
End Term (Implementation and Viva-Voce)	40
Total	**100**

Suggested Readings

1. Lab Manual

Course Code: CBS.534
Course Title: Big Data Analytics and Visualization Lab
Total Hours: 30

L	T	P	Cr
0	0	2	1

Course Objectives:
The lab will help students prepare the big data with pre-procesing analysis and to extract the meaningful data from unstructured data. Help student to develop data visualizations skill and to apply various tools for analysis of structured and unstructured big data.

Learning outcome:
After completion of lab course, students would be able to:
CLO1: Pre-process the un-structured data by various cleaning activities.
CLO2: Convert the un-structured data to structured format.
CLO3: Use Python libraries for analysis and visualisation of data such as PySpark, PyMongo,pandas, numpy and beutifulsoap.

Lab Assignments
Practical will be based on as per the Teaching Learning in the Theory Class**.**

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

Component	**Marks**
Continuous Evaluation	60
End Term (Implementation and Viva-Voce)	40
Total	**100**

Suggested Readings
1. Lab Manual

Course Code: CST.534
Course Title: Internet of Things-Lab
Total Hours: 30

L	T	P	Cr
0	0	2	1

Course Objectives:
The outcome of IOT Lab is to introduce the students to the different IOT technologies. To develop skills that will help the students to develop different IOT applications. To help use different IOT protocols and analysis the data in IOT.

Course Learning Outcomes:
After completion of course, students would be able to:
CLO1: Identify the different technology and develop IoT based applications.
CLO2: Implement IoT applications on different embedded platform.
CLO3: Evaluate the data received through sensors in IOT.

Lab Assignments
Practical will be based on as per the Teaching Learning in the Theory Class.

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

Component	**Marks**
Continuous Evaluation	60
End Term (Implementation and Viva-Voce)	40
Total	**100**

Suggested Readings
1. Lab Manual

Course Code: CBS 626
Course Title: Web Development and Penetration Testing-Lab
Total Hours: 30

L	T	P	Cr
0	0	2	1

Course Objectives:
The objective of the lab course is to provide students with hands-on experience in web development and security practices. Students will be trained to explore web server profiling, intercept and manipulate, identify and exploit vulnerabilities, and demonstrate mitigation techniques for common web attacks.

Course Learning Outcomes:

After completion of course, students would be able to:

CLO1: Apply knowledge of web development concepts and techniques to create secure and functional web applications.

CLO2: Analyze and evaluate web application vulnerabilities and apply appropriate penetration testing methodologies to identify and mitigate them.

CLO3: Demonstrate effective problem-solving and critical thinking skills in identifying and addressing security flaws in web applications through hands-on practical exercises.

Lab Assignments
Practical will be based on as per the Teaching Learning in the Theory Class**.**

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

Component	**Marks**
Continuous Evaluation	60
End Term (Implementation and Viva-Voce)	40
Total	**100**

Suggested Readings

1. Lab Manual

Course Code: CBS.535
Course Title: Digital Forensics Lab
Total Hours: 30

L	T	P	Cr
0	0	2	1

Course Objectives:
The objective of this course is to provide practical exposure of tools used to perform various activities related to different types of digital forensics such as memory forensics, network forensics and web forensics.

Course Learning Outcomes:
After completion of this lab course, students would be able to:
CLO1: Prepare case documents.
CLO2: Setup platform for digital investigation.
CLO3: Acquire and analyse various types of electronic evidences.
CLO4: Analyse Email and web communication headers.

Lab Assignments
Practical will be based on as per the Teaching Learning in the Theory Class**.**

Lab Evaluation:

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

Component	**Marks**
Continuous Evaluation	60
End Term (Implementation and Viva-Voce)	40
Total	**100**

Suggested Readings:

1. Lab Manual

2. Marcella, A. J.(2007), Cyber forensics: A field manual for collecting, examining and preserving evidence of computer crimes. New York: Auerbach publication

Course Code: CBS.536
Course Title: Secure Coding Lab
Total Hours: 30

L	T	P	Cr
0	0	2	1

Course Objectives:
The outcome of this course is to explain the most frequent programming errors leading to software vulnerabilities and identify security problems in software.

Course Learning outcome:
After completion of this lab course, students would be able to:
CLO1: Implement secure programs and list various risks in the software.
CLO2: Classify different errors that lead to vulnerabilities.
CLO3: Analyse various possible security attacks in the programs.

Lab Assignments

Practical will be based on as per the Teaching Learning in the Theory Class**.**

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

Component	**Marks**
Continuous Evaluation	60
End Term (Implementation and Viva-Voce)	40
Total	**100**

Suggested Readings

1. Lab Manual
2. Seacord, R. C. (2013). Secure Coding in C and C++. United States: Addison Wisley Professional.
3. Chess, B., and West J. (2007). Secure Programming with static Analysis. United States: Addison Wisley.

Course Code: CST.536
Course Title: Blockchain Technology Lab
Total Hours: 30

L	T	P	Cr
0	0	2	1

Course Objectives:
The outcome of this course is to introduce students to the concept of Blockchain, crypto primitives, Bitcoin basics, distributed consensus, consensus in Bitcoin, permissioned Blockchain, hyper ledger fabric and various applications where Blockchain is used.

Course Learning Outcomes:
After completion of this lab course, students would be able to:
CLO1: Design the basic concept of Blockchain, Crypto Primitives, Bitcoin Basics
CLO2: Identify the area in which they can apply permission or permission less Blockchain.
CLO3: Apply Block chaining concept in various applications.

Lab Assignments
Practical will be based on as per the Teaching Learning in the Theory Class**.**

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

Component	**Marks**
Continuous Evaluation	60
End Term (Implementation and Viva-Voce)	40
Total	**100**

Suggested Readings

1. Lab Manual
2. Gaur, N., Desrosiers, L., Ramakrishna, V., Novotny, P., Baset, S., & O’Dowd A. (2018). Hands-On Blockchain with Hyperledger: Building decentralized applications with Hyperledger Fabric and Composer. United Kingdom: Packt Publishing Ltd. Packt.
3. Badr, B., Horrocks, R., and Xun(Brian), Wu. (2018). Blockchain By Example: A developer's guide to creating decentralized applications using Bitcoin, Ethereum, and Hyperledger. United Kingdom: Packt Publishing Ltd.

L	T	P	Cr
0	0	2	1

Course Code: CBS.538
Course Title: Quantum Computing & Cryptography Lab
Total Hours: 30

Course Objectives:

To provide one-to-one correspondence between theory and hands-on in terms of in-depth knowledge of fundamentals of Quantum Information Processing. To develop skills with hand-on experience of simulation of quantum computation in order to work in the field of Quantum Information Processing and Cryptography. To acquire deeper understanding to design, develop, and analyse efficient algorithms in the field of Quantum Computing.

Course Learning Outcomes:
At the end of the course the student will be able to:
CLO1: Write a script to simulate qubits, multi-qubit pure and mixed quantum states, the celebrated Bell states and density matrices associated with entangled systems.
CLO2: Write a script to simulate quantum circuits composed of single and multi-qubit quantum gates.
CLO3: Write a script to simulate different measures of entanglement and no locality in pure and mixed two and three-qubit states.
CLO4: Write a script to simulate different noisy channels to analyse the effect of noise on entanglement and efficiency of a protocol.
CLO5: Simulate different quantum information processing protocols such as teleportation, dense coding, and Secret Sharing.

Lab Assignments
Practical will be based on as per the Teaching Learning in the Theory Class**.**

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

Component	**Marks**
Continuous Evaluation	60
End Term (Implementation and Viva-Voce)	40
Total	**100**

Suggested Readings

1. Lab Manual

Course Code: CST.517
Course Title: Machine Learning Lab
Total Hours: 30

L	T	P	Cr
0	0	2	1

Course Objectives:

The objectives of the Machine Learning Lab course 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.

Course Learning Outcomes::

After completion of course, students would be able to:
CLO1: Review some common Machine Learning algorithms and their limitations.
CLO2: Apply common Machine Learning algorithms in practice and implementing the same.
CLO3: Perform experiments in Machine Learning using real-world data.

Lab Assignments

Practical will be based on as per the Teaching Learning in the Theory Class.

Lab Evaluation:

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

Component	**Marks**
Continuous Evaluation	60
End Term (Implementation and Viva-Voce)	40
Total	**100**

Suggested Readings:

1. Lab Manual
2. Kumar, U.D., and Pradhan, M. (2019). Machine Learning using Python. Wiley

Value Added Course
(For other departments only as per the availability of faculty)

Course Code: CST.505
Course Title: Basics of Machine Learning
Total Hours: 30

L	T	P	Cr
2	0	0	2

Course Objectives:

The objective of this course is to develop a strong understanding of the issues and challenges associated with machine learning. It aims to provide students with insights into the strengths and limitations of various popular machine learning approaches. The course also focuses on enabling students to apply appropriate machine learning techniques for effective data handling and knowledge extraction. Furthermore, it equips learners with the skills to evaluate the performance of algorithms and design solutions for real-world applications.

Course Learning Outcomes:

At the end of this course, students will be able to:
CLO1: Recognize the characteristics of machine learning strategies
CLO2: Pre-process the data before applying to any real-world problem and can evaluate its performance
CLO3: Apply various supervised learning methods to appropriate problems
CLO4:. Identify and integrate more than one technique to enhance the performance of learning.

Units/Hours	Contents/ Activities	Mapping with Course Learning Outcome
Unit I **8Hours**	**Introduction**: Brief Introduction to Machine Learning, History and background of History and background of AI and ML, Comparison of AI, ML and DL, Supervised Learning, Unsupervised Learning, Reinforcement Learning, Examples of various Learning Paradigms	**CLO 1**
	Learning Activities: Assignment based learning	
Unit II **7 Hours**	Python Ecosystem for ML: Data loading for ML Projects, understanding data with Statistics, Understanding data with visualization, Pre-processing and feature extraction	**CLO 2**
	Learning Activities: Implementation & demonstration	
Unit III **8 Hours**	Machine Learning patterns Introduction: - Classification (Linear Regression, Logistic Regression, Support Vector Machine, Naïve Bayes, Decision Tree, Random Forest) Clustering.	**CLO 3**
	Learning Activities: Real time examples and implementation.	

Unit IV **7 Hours**	**Recent Trends:** Recent Trends and Applications of Machine Learning in different fields.	**CLO 4**
	Learning Activities: Presentations	

Transactional Modes:

- Lecture
- Blended Learning
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Marc Peter Deisenroth, A. Aldo Faisal, Cheng Soon Ong, “Mathematics for Machine Learning”, Cambridge University Press, 2019.
2. Tom M. Mitchell, ―Machine Learning, McGraw-Hill Education (India) Private Limited, 2013.
3. Ethem Alpaydin,"Introduction to Machine Learning”, MIT Press, Prentice Hall of India, Third Edition 2014.

Course Code: CBS.504
Course Title: Report writing using LaTeX
Total Hours: 32

L	T	P	Cr
2	0	0	2

Course Objectives:
The objective of this course is to equip students with the fundamental knowledge and practical skills required to create professional and structured documents using LaTeX. It aims to familiarize students with the basic commands and environments in LaTeX, enabling them to write articles, reports, theses, and other academic or technical documents. The course also focuses on building the capability to script various types of documents and integrate elements such as tables, figures, equations, and references. Additionally, it encourages the development of problem-solving skills to debug and troubleshoot LaTeX compilation issues effectively.

Course Learning Outcomes:
After the completion of course, participants will be able to:
CLO1: Use the basic commands in Latex.
CLO2: Develop scripts in Latex for different type of documents.
CLO3: Illustrate troubleshooting in the latex scripts.

Units/Hours	Contents	Mapping with Course Learning Outcome
I **8 Hours**	**Latex Introduction:** Installing and setting Latex environment in Windows and Linux. **Document Structure:** Essential in preparing the structure of documents, Creating Titles at different levels, Sections, Labelling and preparing Table of Contents.	**CLO-1**
	Activities: Live Demonstration of LaTeX scripts. Assignment to write the LaTeX scripts.	
II **8 Hours**	**Formatting Text:** Font Effects, Colored Text, Font Size, Bullets and lists, Comments, Spacing and Special Characters.	**CLO-1** **CLO-2**
	Activities: Live Demonstration of LaTeX scripts. Assignment to write the LaTeX scripts.	
III **8 Hours**	**Tables:** Working with tables, Styles, Borders, Wrapping, Inserting new rows columns and caption of Tables. **Figures:** Working with Figures, Formatting of Figures, caption, Alignment and wrapping Text around figures.	**CLO-1** **CLO-2**
	Activities: Live Demonstration of LaTeX script. Assignment to write the LaTeX scripts.	

IV **8 Hours**	**Equation:** Inserting Equation, Mathematical Symbols, Fractions, Roots, Sums & Integrals and Greek Letters. **References:** BibTeX File, Inserting the bibliography, Citing References, Styles of References	**CLO-1,** **CLO-2** **CLO-3**
	Activities: Live Demonstration of LaTeX scripts. Assignment to write the LaTeX scripts.	

Transactional Modes:

- Lecture
- Peer Learning/Teaching
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Lamport, L. (2014), Latex A document preparation system. New York: Adisson Wesley Publishing Company.
2. Helmut Kopka & Patrick W. Daly(2004): A Guide to LATEX and Electronic Publishing (Fourth Edition), Addison-Wesley Longman Ltd. Chapters: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 14, 15
3. Kotwiz. S. (2015). Latex Cook Book. United Kingdom: Packt Publishing Lmt.
4. Nicola Louise Cecilia Talbot. (2013). Using LaTeX to Write a PhD Thesis, Dickimaw Books.
5. Research Articles from SCI & Scopus indexed Journals.

Value Added Course

As per the availability of faculty

Course Code: CST.XXX
Course Title: AI for Education
Total Hours: 30

L	T	P	Cr
2	0	0	2

Course Objectives:
This course aims to familiarize students and educators with Artificial Intelligence (AI) tools that enhance teaching, learning, and research practices. It provides hands-on experience with AI-powered applications for content creation, personalized learning, assessment, academic writing, and research productivity. The course encourages ethical and effective integration of AI into academic environments while promoting critical thinking about the use and limitations of AI in education.

Course Learning Outcomes:
After the completion of course, participants will be able to:

CLO1: Understand the fundamentals of AI and its relevance in the education sector.
CLO2: Use AI tools for teaching support, student engagement, and content creation.
CLO3: Employ AI-driven platforms for academic writing, citation management, and research enhancement.
CLO4: Apply AI-based tools for assessment, feedback, and personalization of learning.
CLO5: Evaluate ethical and responsible use of AI in education.

Units/Hours	Contents	Mapping with Course Learning Outcome
I **08 Hours**	**Introduction to AI in Education (Theory + Demo)** Overview of AI and Machine Learning concepts, Role of AI in modern education systems, Use cases of AI for teachers, students, and researchers, Types of AI tools: Generative AI, Predictive AI, and Analytical AI, Responsible and ethical use of AI in academics	**CLO1, CLO5**
	Activities: Live demonstration of AI use cases in education, Assignment on identifying 5 AI tools with academic use cases	
II **08 Hours**	**AI Tools for Teaching and Learning** Content creation tools: ChatGPT, Copilot, Canva AI, Tome AI, Lecture generation & presentation tools: Gamma, SlidesAI, AI tools for student engagement: Mentimeter, Curipod, EdPuzzle, ClassPoint, Personalized learning apps:	**CLO2, CLO4, CLO5**

	Scribehow, Diffit, MagicSchool.ai, AI-driven LMS integrations and virtual assistants	
	Activities: Live demonstration of AI tools for lesson planning and student engagement, Assignment to design a 3-slide AI-generated micro lesson with quiz	
III **08 Hours**	**AI Tools for Students and Academic Writing** Note-taking tools: Otter.ai, Notion AI, Grammar and writing enhancement: Grammarly, Quillbot, Hemingway, Summarization and reading tools: Scholarcy, TLDRthis, Reference and citation: EndNote, Zotero, Mendeley (with AI plugins), Avoiding plagiarism and responsible AI use in writing	**CLO3, CLO5**
	Activities: Live demonstration of AI tools for writing and referencing, Assignment to write an academic paragraph using AI tools with proper citations	
IV **08 Hours**	**AI for Research and Assessment** Literature review tools: Elicit, Research Rabbit, Connected Papers, Data analysis and visualization: ChatGPT Code Interpreter, SciSpace, Wolfram Alpha, Assessment generation: QuestionWell, Testportal, Formative, Feedback tools and rubrics generation using AI, Limitations and biases in AI tools for research and evaluation, Introduction to Prompt Engineering.	**CLO3, CLO4, CLO5**
	Activities: Live demonstration of AI tools for research and assessment, Assignment to create a mini research workflow using two or more AI tools	

Transactional Modes:

- Lecture
- Peer Learning/Teaching
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Holmes, W., Bialik, M., & Fadel, C. (2019). *Artificial intelligence in education: Promises and implications for teaching and learning*. Center for Curriculum Redesign.

2. Luckin, R. (2021). *AI in education: A guide for students and teachers*. Routledge.

3. Fitzpatrick, D., Fox, A., & Weinstein, B. (2023). *The AI classroom: The ultimate guide to artificial intelligence in education*. IMPress.

4. Huang, R., & Yang, J. (2023). *Artificial intelligence for education: Technologies and applications*. Springer.

SEMESTER –III

Course Code: CBS.551
Course Title: Biometric Security
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives: The outcome of this course is to introduce students to the concept of biometric security, explore different biometric modalities and their characteristics. Design, implementation, and evaluate of biometric systems. Analyze the vulnerabilities and threats associated with biometric security, learn about the techniques for enhancing the security of biometric systems and know the ethical and legal issues related to biometric security.

Course Learning Outcomes:
After completion of course, students would be able to:
CLO1: Describe the various modules constituting a bio-metric system. Compare and contrast the different bio-metric traits and appreciate their relative significance.
CLO2: Classify the different feature sets used to represent some of the popular bio-metric traits.
CLO3: Evaluate and design security systems incorporating bio-metrics.
CLO4: Discuss methods to enhance security of biometrics, ethical and legal issues related to biometric security

Units/Hours	Contents	Mapping with Course Learning Outcome
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.	**CLO1**
	Activities : Assignments and Problem based Exercise	
II **15 Hours**	Introduction to image segmentation and Image feature extraction. 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.	**CLO2**
	Activities: Hands on training using open source software tools.	
III **21 Hours**	Biometric System Architecture: Sensor technologies and data acquisition, Feature extraction and representation, Matching algorithms and decision-making, Template storage and managemen, System integration and deployment. Biometric System Evaluation: Performance metrics and evaluation protocols, Receiver Operating Characteristic (ROC)	**CLO1**

	analysis, Error types and error rates, Data collection and benchmarking	
	Activities: Group based project development.	
IV **15 Hours**	Vulnerabilities and Attacks: Spoofing and presentation attacks, Biometric template security and storage, Biometric data leakage and identity theft, Impersonation attacks and countermeasures. Enhancing Biometric Security: Biometric cryptosystems: Cancelable biometrics, Liveness detection and anti-spoofing techniques, Template protection and secure storage, Continuous authentication and adaptive systems Ethical and Legal Issues: Privacy concerns and data protection, Biometric data management and retention policies, Biometric regulations and standards, Social implications and public perception	**CLO3**
	Activities: Case studies.	

Transactional Modes:

- Lecture
- Experimentation
- Case study
- Demonstration
- Discussion
- Problem solving
- Online Teaching Tools

Suggested Readings:

1. Jain, A.K., Flynn, P., and Ross, A.A. (2008) Handbook of Biometrics: Springer.
2. Kumar, A., and Zhang, D. (2005) Biometric Systems: Technology, Design and Performance Evaluation, Springer.
3. Zhang, D., Sun, F., and Toh, K.A. (2005) Multimodal Biometrics: Principles and Applications, Springer.
4. Jain, A.K., Jaccard, J., and Nandakumar, K. (2017) Biometric Security and Privacy: Opportunities & Challenges in the Big Data Era, Springer.
5. Gonzalez, R. C., and Woods, R. E. (2018). Digital Image Processing India: Person Education.
6. Research Articles from SCI & Scopus indexed Journals.

Course Code: CST.552
Course Title: Data Warehousing and Data Mining
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:

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

Course Learning Outcomes:

After completion of course, students would be able to:
CLO1: Discuss different sequential pattern algorithms.
CLO2: Apply the techniques to extract patterns from time series data and their applications in real world.
CLO3: Examine Graph mining algorithms to Web mining.
CLO4: Design the computing framework for Big Data.

Units/Hours	Contents	Mapping with Course Learning Outcome
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;	**CLO-1** **CLO-4**
	Activities: 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.	
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.	**CLO-1**
	Activities: Assignment based learning, Exercise based learning.	
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.	**CLO-2**

	Activities: Case based study and Group discussion for the prediction of solutions for real time problems.	
IV **15 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.	**CLO-3** **CLO-4**
	Activities: Student presentation, Class discussion on different types of mining for the solution of real world problem.	

Transactional Modes:

- Lecture cum Demonstration
- Peer Learning/Teaching
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Han, J., and Kamber, M., (2011). Data Mining Concepts and Techniques. Elsevier Publication.
2. Tan, P., Kumar, V., & Steinbach M. (2016). Introduction to Data Minings. New Delhi: Pearson Education.
3. Dong, G., and Pei, J. (2007). Sequence Data Mining. New York: Springer.
4. Han, Jiawei, Kamber, Micheline, Pei, Jian. (2012). Data mining: Concepts and techniques, USA: Morgan Kaufman publishers.
5. Kantardzic, Mehmed. (2011). Data mining: concepts, models, methods and algorithms. New Jersey: John, Wiley & sons.
6. Research Articles from SCI & Scopus indexed Journals.

Course Code: CBS.526
Course Title: Security Auditing and Risk Management
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:
The objective of this course is to introduce students to the fundamental concepts of risk management in the context of information security and organizational operations. It aims to help students define and distinguish between various components of contingency planning, such as Incident Response Planning (IRP), Disaster Recovery Planning (DRP), and Business Continuity Planning (BCP). The course is designed to guide students in integrating these components into a comprehensive and coherent strategy that supports sustained organizational functionality. Additionally, students will learn to evaluate different incident response options and develop a practical Incident Response Plan tailored to real-world organizational needs.

Course Learning Outcomes:
After completion of course, students would be able to:
CLO1: State contingency strategies including data backup and recovery and alternate site selection for business resumption planning
CLO2: Describe the escalation process from incident to disaster in case of security disaster.
CLO3: Design a Disaster Recovery Plan for sustained organizational operations.
CLO4: Design a Business Continuity Plan for sustained organizational operations.

Units/Hours	Contents	Mapping with Course Learning Outcome
I **15 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.	**CLO1**
	Activities: Group discussion and Case study.	
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.	**CLO2**
	Activities: Group Discussion and panel Discussion.	

III **14 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, modernization and migration management, 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.	**CLO3** **CLO4**
	Activities: Group Discussion and panel Discussion.	
IV **16 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 (needto-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	**CLO4**
	Activities: Case study of threat and vulnerability assessment.	

Transactional Modes:

- Lecture
- Case Studies
- Collaborative
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Information Security Management Principles-- David Alexander, Amanda Finch, David Sutton,Andy Taylor [BCS Learning 3rd Edition, 2020]
2. IT Security and Risk Management -- J. Slay and A. Koronios[Wiley 3rd Edition 2012]

3. Information Security Management Handbook-- Harold F. Tipton and Micki Krause [Auerbach Publications, 6th edition 2019]
4. Mark Talabis, Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis, Syngress; 1 edition, ISBN: 978-1-59749-735-0, 2012.
5. Information Technology Control and Audit, Fourth Edition, Sandra Senft, Frederick Gallegos, Aleksandra Davis, CRC Press, 2012.

Course Code: CST.554
Course Title: Mobile security & Service
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:

This course presents the three main mobile platforms and their ecosystems, namely Android, iOS, and PhoneGap/Web OS. It explores emerging technologies and tools used to design and implement feature-rich mobile applications for smartphones and tablets

Course Learning Outcomes:

After completion of course, students would be able to:

CLO1: Explain the fundamentals, frameworks, and development lifecycle of mobile application platforms including iOS, Android, and PhoneGap.

CLO2: Identify the target platform and users.

CLO3: Design and develop a mobile application prototype in one of the platforms (challenge project).

Units/Hours	Contents	Mapping with Course Learning Outcome
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.	CLO1
	Activities: Group Discussion, Case studies.	
II 14 Hours	Mobile Platform Development Fundamentals, Mobile Application Lifecycle, Architecture & Application Structure, SDKs & Development Environments, Mobile Components: Activities, Intents, Services, Broadcast Receivers, Content Providers, APIs & SDK Tools, Emulator Setup & Debugging, Mobile UI Design Principles, Security Models of Android, iOS, PhoneGap, Sandboxing, Permissions, App Signing, Mobile Threats, OWASP Mobile Top 10, Secure Coding Practices, Assignment-Based Learning, Live Demonstration, Comparative Analysis, Security Architecture Analysis,	CLO1, CLO2
III 15 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	CLO2

	Alarms, Graphics, Performance and Multithreading, Graphics and UI Performance, Android Graphics.	
	Activities: Implementation based Learning, Live Demonstrations of Android Notifications and Graphics	
IV **15 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.	**CLO3**
	Activities: Case studies on recent trends, Presentations by students, Assignment based Learning.	

Transactional Modes:

- Lecture cum Demonstration
- Peer Learning/Teaching
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Lee, W. (2012). Beginning Android TM 4 Application Development. United Sates: John Wiley & Sons.
2. B'far, Reza. (2013). Mobile computing principles: Designing and developing mobile applications with UML and XML. New Delhi: Cambridge university press.
3. Research Articles from SCI & Scopus indexed Journals.

Course Code: CBS 632
Course Title: Deep Learning
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:
The objective of this course is to introduce students to the fundamental concepts and principles of Neural Networks and Deep Learning. Students will gain an understanding of how to match deep networks to appropriate problems and explore the practical applications of Deep Learning across various domains. The course also aims to provide a comprehensive understanding of different Deep Learning architectures, and students will have the opportunity to implement these architectures to solve real-world problems.

Course Learning Outcomes:
After completion of course, students would be able to:
CLO1: Understand the role of Deep learning in Various Applications.
CLO2: To design and implement Various Deep Learning Architecture.
CLO3: Critically Analyse Different Deep Learning Models in various Projects.
CLO4: To know about applications of Deep Learning in NLP and Sequence Modelling

Units/Hours	Contents	Mapping with Course Learning Outcome
I **14 Hours**	Feed Forward Neural Networks, Gradient Descent, Back Propagation Algorithm, Vanishing, Gradient problem, Mitigation Defining Deep Learning, Common Architecture of Deep Networks, Building Blocks of Deep Networks: RBM, Autoencoders, Variational Autoencoders	**CLO1, CLO2**
	Activities: Discussion of role of Neural Networks and Compression of features using Autoencoders. Practical – Installation of TensorFlow and Keras.	
II **15 Hours**	**Unsupervised Pretrained Networks:** Deep Belief Network, Generative Adversarial Network. **Convolutional Neural Networks(CNN):** General Architecture, Input Layers, Convolutional Layers, Pooling Layers, Fully Connected Layers. **Recurrent Neural Networks:** General Architecture, Modelling with Time Dimensions, LSTM Network, Recursive Neural Network: Network Architecture, Varieties of Recursive Neural Networks	**CLO2**
	Activities: Discussion of role of CNN, RNN in Machine Learning. Assignment based learning for Concept of convolution and need for Pooling, Implementation of CNN and RNN with Tensor Flow	

III **16 Hours**	Matching Deep network for Right Problem, Modelling text Data with RNN, Implementation of LSTM and GRU layer. Generative RNN, Using RNN dropout to fight Overfitting. Using Bi-directional RNNs, Using Regularisation Modelling Sequencing Data Using RNN. Implementing 1D Convolution and pooling for sequencing Data, Combining CNNs and RNNs for processing long Sequence. Training and evaluation of Model, Large Language Models: BERT and GPT.	**CLO3,** **CLO4**
	Activities: Implementation of algorithms and assignment based learning.	
IV **15 Hours**	Tunning CNN: CNN Architecture Patterns, Configuring Convolution Layers, Configuring Pooling Layers and Transfer Learning. Tunning RNN: Preparing Network input data and Input Layer, Output layer and Run Output Layer, Training the Network, Common Issues with LSTM, Padding and Masking, Scoring with Masking.	**CLO4**
	Activities: Implementation and solution of CNN and RNN, case study of recent trends in Deep Learning.	

Transactional Modes:

- Lecture
- Google Co-lab
- Collaborative Learning
- Peer Learning/Teaching
- Github/Kaggle

Suggested Readings:

1. Ian Good Fellow, Yoshua Bengio, Aaron Courville, “Deep Learning”, MIT Press, 2020.
2. Francois Chollet, “Deep Learning with Python”, Manning Publications, 2021.
3. Phil Kim, “Matlab Deep Learning: With Machine Learning, Neural Networks and Artificial Intelligence”, Apress , 2017.
4. Ragav Venkatesan, Baoxin Li, “Convolutional Neural Networks in Visual Computing”, CRC Press, 2018.
5. Navin Kumar Manaswi, “Deep Learning with Applications Using Python”, Apress, 2018.
6. Joshua F. Wiley, “R Deep Learning Essentials”, Packt Publications, 2016.
7. Research Articles from SCI & Scopus indexed Journals.

Course Code: CBS.552
Course Title: Cyber Threat Intelligence
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:

The objective of this course is to introduce students to explain the cyber threats and cyber threat intelligence requirements. Classify cyber threat information and examine the potential for incidents and, provide more thoughtful responses.

Course Learning Outcomes:

After completion of course, students would be able to:
CLO1: Describe different Cyber Threat.
CLO2: Explain technique to Develop Cyber Threat Intelligence Requirements.
CLO3: Analyze and Disseminate Cyber Threat Intelligence.

Units/Hours	Contents	Mapping with Course Learning Outcome
I **16 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	**CLO1**
	Activities: Case Study and Group Discussion.	
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	**CLO2**
	Activities: Case study of real time social media cases.	
III **14 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. Analysing and Disseminating Cyber Threat Intelligence: Information versus Intelligence, Validation and Prioritization: Risk scores, Tags for context, Human assessment.	**CLO3**

	Interpretation and Analysis: Reports, Analyst skills, Intelligence platform, Customization. Dissemination: Automated feeds and APIs, Searchable knowledge base, Tailored reports.	
	Activities: Case study of real time social media cases.	
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.	**CLO3**
	Activities: Flip Learning with Case studies of above concepts.	

Transactional Modes:

- Lecture cum Demonstration
- Cooperative learning
- Flipped classroom
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Friedman, J., and Bouchard, M., CISSP. Foreword by Watters, J. P., (1997). Definitive Guide to Cyber Threat Intelligence. Maryland: Cyber Edge Group, LLC.
2. Roberts, S. J., and Brown, R. (2017). Intelligence- Driven Incident Response: Outwitting the Adversary. California: O'Reilly Media.
3. Bautista, W. (2018). *Practical cyber intelligence: how action-based intelligence can be an effective response to incidents*. Packt Publishing Ltd.
4. Pace, C. (2018). The threat intelligence handbook: A practical guide for security teams to unlocking the power of intelligence. *Annapolis, CyberEdge Group*.
5. Bazzell, M. (2016). *Open source intelligence techniques: resources for searching and analyzing online information*. CreateSpace Independent Publishing Platform.
6. Dalziel, H., (2014). How to Define and Build an Effective Cyber Threat Intelligence Capability. Elsevier Science & Technology.
7. Robertson, J., Diab, A., Marin, E., Nunes, E., Paliath, V., Shakarian, J., & Shakarian, P., (2017). DarkWeb Cyber Threat Intelligence Mining. New Delhi: Cambridge University Press.
8. Gourley, B., (2014). The Cyber Threat. United States: Createspace Independent Pub.
9. Research Articles from SCI & Scopus indexed Journals.

Course Code: CST.556
Course Title: Cost Management of Engineering Projects
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives

This course provides students with skills and knowledge of cost management of engineering projects. The course will enable students to understand the key components of engineering project.

Course Learning Outcomes:

After the completion of the course the students will be able to

CLO1: Employ their knowledge and skills together to understand the basics of a successful project.
CLO2: Explain the cost behaviour and profit planning.
CLO3: Compare various quantitative methods for cost management.

Units/Hours	Contents	Mapping with Course Learning Outcome
I **16 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.	**CLO1**
	Activities: Numerical Example for above concepts.	
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.	**CLO1** **CLO2**
	Activities: Case study of IT Companies.	
III **14 Hours**	Cost Behaviour 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	**CLO-3**

	Resource Planning, Total Quality Management and Theory of constraints.	
	Activities: Case study and Numerical example to understand the above theory.	
IV **16 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.	**CLO-4**
	Activities: Case study and Numerical Example for better understanding.	

Transactional Modes:

- Lecture
- E-tutorial
- Problem Solving
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Horngren, C. T., and Datar, S. M. (2017). Cost Accounting a Managerial Emphasis. New Delhi: Pearson Education.
2. Riahi-Belkaoui, A. (2001). Advanced Management Accounting. California: Greenwood Publication Group.
3. Kaplan, R. S., and Alkinson, A. A. (1998). Management Accounting. United States: Prentice Hall.
4. Bhattacharya, A. K. (2012). Principles & Practices of Cost Accounting. Allahabad, A. H. Wheeler publisher.
5. Vohra, N. D. (2017). Quantitative Techniques in Management. New Delhi: Tata McGraw Hill Education.
6. Rao, Thukaram M.E. (2011). Cost and management accounting. New Delhi: New age international publishers.
7. Research Articles from SCI & Scopus indexed Journals.

Course Code: CBS.553
Course Title: Cyber Law
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:
The outcome 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 Learning Outcomes:
After completion of course, students would be able to:
CLO1: Analyse fundamentals of Cyber Law.
CLO2: Discuss IT Act & its Amendments.
CLO3: Relate Cyber laws with security incidents.

Units/Hours	Contents	Mapping with Course Learning Outcome
I **13 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.	**CLO1**
	Activities: Case Studies on Jurisdiction	
II **15 Hours**	Electronic Commerce, Cyber Contract, Intellectual Property Rights and Cyber Laws. UNCITRAL Model Law, Digital Signature and Digital Signature Certificates, E-Governance and Records.	**CLO2**
	Activities: Brainstorming Sessions on Significance of UNCITRAL in day to day life of a common man.	
III **17 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.	**CLO2** **CLO3**
	Activities: Assignment based learning, Demonstration of Entanglement and Non-locality through animated videos.	
IV **15 Hours**	Obscenity and Pornography, Internet and potential of Obscenity, International and National Instruments on Obscenity & Pornography, Child Pornography, Important Case Studies.	**CLO3**
	Activities: Exericses and problem solving skills on cybercrimes.	

Transactional Modes:

- Lecture cum Demonstration
- Peer Learning/Teaching
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Ahmad, F. (2015). Cyber Law in India, Faridabad: New era law publications.
2. Sharma, J.P., Kanojia, S. (2016). Cyber Laws, New Delhi: Ane Books Pvt Ltd.
3. Chander, H. (2012). Cyber Laws and IT Protection. New Delhi: Prentice Hall India Learning Private Limited.
4. Justice Yatindra Singh. (2016). Cyber Laws. New Delhi: Universal Law Publishing Co.
5. Chaubey, R.K. (2012). An Introduction to cyber-crime and cyber law, Kolkata: Kamal Law House.
6. Tiwari, G. (2014). Understanding Laws: Cyber Laws & Cyber Crimes. New York: Lexis Nexis.
7. Seth, K. (2013). Justice Altamas Kabir, Computers Internet and New Technology Laws. New York: Lexis Nexis.
8. Research Articles from SCI & Scopus indexed Journals.

Course Code: CST.557
Course Title: Software Metrics
Total Hours: 60

L	T	P	Cr
4	0	0	4

Course Objectives:

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

Course Learning Outcomes:

After completion of course, students would be able to:

CLO1: Explain the role of software Metrics in Industry size software

CLO2: Prepare empirical investigation of software for a quality measurement

CLO3: Examine software reliability and problem solving by designing and selecting software reliability models.

Units/Hours	Contents	Mapping with Course Learning Outcome
I **15 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.	**CLO1**
	Activities: Case study and Group Discussion on OO methodology.	
II **16 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.	**CLO1** **CLO2**
	Activities: Case study with Understand and Metrics Tools.	
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, Aspects of Quality Measurements, Maintainability Measurements, Usability and Security Measurements.	**CLO2**
	Activities: Case study with Bugzila and JEERA tools.	

IV **13 Hours**	Measuring software Reliability: Concepts and definitions, Software reliability models and metrics, Fundamentals of software reliability engineering (SRE), Reliability management model.	**CLO3**
	Activities: Case study with Bugzilla and JEERA tools.	

Transactional Modes:

- Lecture cum Demonstration
- Peer Learning/Teaching
- E-tutorial
- Self-Learning
- Online Teaching Tools

Suggested Readings:

1. Fenton, N. E. and Pfleeger, S. L. (1997). Software Metrics: A Rigorous and Practical Approach. New York: International Thomson Computer Press.
2. Kan, S. H. (2002). Metrics and Models in Software Quality Engineering. United States: Addison-Wesley Professional.
3. Anirban, B. (2015). Software Quality Assurance, Testing and Metrics. United States: Prentice Hall India Learning.
4. Tian, Jeff. (2010). Software quality engineering: Testing, quality assurance and quantifiable improvement. New Delhi: Wiley India.
5. Stephen H Khan: Metrics and Models in Software Quality Engineering, Pearson 2nd edition 2013
6. Research Articles from SCI & Scopus indexed Journals.

L	T	P	Cr
L	**T**	**P**	**Cr**
0	0	20	10

Course Code: CBS.600
Course Title: Dissertation Part-I

Course Objectives:

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 Learning Outcomes:

CLO1: The students would present their work to the Evaluation Committee (constituted as per the university rules). The evaluation criteria shall be as detailed below:

SEMESTER –IV

Course Code: CBS.600
Course Title: Dissertation Part-II

L	T	P	Cr
0	0	32	16

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 Learning 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 By	Maximum Marks	Evaluation Criteria
External expert, HoD and senior-most faculty of the department	50	Dissertation report (30), presentation (10), final viva-voce (10)
Supervisor	50	Continuous assessment (regularity in work, mid-term evaluation) dissertation report, presentation, final viva-voce
Total	100	