FORENSIC SCIENCE AND DIGITAL FORENSICS

Course Code	**22SFC13**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	3:0:2	SEE Marks	50
Total Hours of Pedagogy	50	Total Marks	100
Credits	04	Exam Hours	03

Course Learning objectives:
- Learn basics of Forensic science, Computer Crime and analysis of cyber Criminalistics.
- Learn working of corporate investigations, Email and web forensics and network forensics.
- Learn E-discovery, guidelines and standards, E-evidence, tools and environment.

Module-1
Forensic 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.

Teaching-Learning Process	**Chalk and Talk method /PPT/ Case study/Web contents**

Module-2
Digital forensic: Understanding computer forensics, computer forensics versus other related disciplines, A brief History of computer Forensics, Understanding case laws, Developing computer forensics resources, Preparing for computer investigations, Understanding law enforcement agency investigations, Following the legal process, Understanding corporate investigations, Establishing company policies, Displaying warning Banners.

Teaching-Learning Process	**Chalk and Talk method /PPT/ Case study/Web contents**

Module-3
Incident- Cyber Crime Scene Analysis: Discuss the various court orders etc., methods to search and seizure electronic evidence, retrieved and un-retrieved communications

Teaching-Learning Process	**Chalk and Talk method /PPT/ Case study/Web contents**

Module-4
Data Forensics: Recovering deleted files and deleted partitions, deleted file recovery tools deleted partitioned recovery tools, data acquisition and duplication, data acquisition tools hardware tools, backing up and duplicating data.

Teaching-Learning Process	**Chalk and talk method / PowerPoint Presentation/Case study /Web link**

Module-5
Digital Forensics Introduction to Digital Forensics, Forensic Software and Hardware, Analysis and Advanced Tools, Forensic Technology and Practices, Forensic Ballistics and Photography, Face, Iris and Fingerprint Recognition, Audio Video Analysis, Windows System Forensics, Linux System Forensics, WIFI Security (War-driving), Network Forensics, Mobile Forensics, Cloud Forensics.

Teaching-Learning Process	**Chalk and Talk method /PPT/ Case study/Web contents/Android and IOS**

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Three Unit Tests each of **20 Marks**
2. Two assignments each of **20 Marks** or **one Skill Development Activity of 40 marks** to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:

1. The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
2. The question paper will have ten full questions carrying equal marks.
3. Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
4. Each full question will have a sub-question covering all the topics under a module.
5. The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:

Text Books

1. *Cory Altheide, Harlan Carvey, Digital Forensics with Open Source Tools*, Syngress imprint of Elsevier.

   Reference Books:

   1. Guide to Computer Forensics and Investigations, Bill Nelson, Amelia Phillips, Christopher Steuart, Fourth Edition, Course Technology

2. *Digital forensics: Digital evidence in criminal investigation,* Angus M.Marshall, John – Wiley and Sons, 2008.

   3. Cybercrime and Digital Forenscis, , Anthony Reyes, Jack Wiles, Syngress Publishers, Elsevier 2007

4. *The Basics of Digital Forensics,* John Sammons, Elsevier 2012

Web links and Video Lectures (e-Resources):

- https://www.youtube.com/watch?v=7I-dcPi4NNE
- https://www.youtube.com/watch?v=s01A-yqOby8

Skill Development Activities Suggested

The students with the help of the course teacher can take up relevant technical –activities which will enhance their skill. The prepared report shall be evaluated for CIE marks.

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Demonstrate the relevant codes of ethics(can be attained through assignment or CIE)	L3
CO2	Explain Computer forensics and digital detective and various processes, policies and procedures concepts.	L2
CO3	Explain E-discovery, guidelines and standards, E-evidence, tools and environment.	L2
CO4	Demonstrate Email and web forensics and network forensics. (can be attained through assignment or CIE)	L3

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	Po1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
3	Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.	PO3
4	Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.	PO4
5	Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations	PO5
6	The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering and business practices.	PO6
7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9
10	Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.	PO10
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.	PO11
12	Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.	PO12

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1								X				X
CO2	X											
CO3		X				X						
CO4				X						X		

SECURITY THREATS AND VULNERABILITIES

Course Code	**22SFC14**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	2:0:2	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:
- Define the different threats identity processes.
- Explain how to find the vulnerabilities in different application
- Able to write their code for vulnerable applications.
- Demostrate the Use of Agent Technology for Intrusion Detection, CSIRTs

Module-1

Threats and Vulnerabilities to Information and Computing Infrastructures: Internal Security Threats, Cyber Physical Security Threats, Fixed-Line Telephone System Vulnerabilities, E-Mail Threats and Vulnerabilities, E-Commerce Vulnerabilities, Hacking Techniques in Wired Networks , Hacking Techniques in Wireless Networks, Computer Viruses and Worms, Trojan Horse Programs, Hoax Viruses and Virus Alerts, Hostile Java Applets, Spyware.

Teaching-Learning Process	**Chalk and Talk method /PPT/ Case study/Web contents/Malwares**

Module-2

Wireless Threats and Attacks: Wireless Threats and Attacks, WEP Security, Bluetooth Security, Cracking WEP, Denial of Service Attacks, Network Attacks, Fault Attacks, Side Channel Attacks.

Teaching-Learning Process	**Chalk and Talk method /PPT/ Case study/Web contents**

Module-3

Prevention: Keeping the Hackers and Crackers at Bay RFID and Security ,Cryptographic Privacy Protection Techniques, Cryptographic Hardware Security Modules, Smart Card Security, Client-Side Security, Server-Side Security ,Protecting Web Sites, Database Security, Medical Records Security, Access Control: Principles and Solutions, Password Authentication ,Computer and Network Authentication, Antivirus Technology, Biometric Basics and Biometric Authentication.

Teaching-Learning Process	**Chalk and Talk method /PPT/ Case study/Web contents**

Module-4

Detection and Recovery: Intrusion Detection Systems Basics, Host-Based Intrusion Detection Systems , Network-Based Intrusion Detection Systems, Use of Agent Technology for Intrusion Detection, Contingency Planning Management, Computer Security Incident Response Teams (CSIRTs) , Implementing a Security Awareness Program, Risk Assessment for Risk Management, Security Insurance and Best Practices. Auditing Information Systems Security, Evidence Collection and Analysis Tools, Information Leakage: Detection and Countermeasures.

Teaching-Learning Process	**Chalk and Talk method /PPT/ Case study/Web contents**

Module-5

Host-level Threats and Vulnerabilities-Malware: Trojan Horse, Spyware, Worms/Viruses Eavesdropping, Job Faults. Infrastructure, Level Threats and Vulnerabilities: Network-Level Threats and Vulnerabilities, Grid Computing, Threats and Vulnerabilities, Storage Threats and Vulnerabilities.

Teaching-Learning Process	**Chalk and Talk method /PPT/ Case study/Web contents**

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Three Unit Tests each of **20 Marks**
2. Two assignments each of **20 Marks** or **one Skill Development Activity of 40 marks** to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:

1. The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
2. The question paper will have ten full questions carrying equal marks.
3. Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
4. Each full question will have a sub-question covering all the topics under a module.
5. The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:

Text Books

1. *Algorithmic Cryptanalysis ,* Antoine Joux , Chapman & Hall/CRC Cryptography and Series, 2009
2. *Number Theory for Computing .* Song Y Yang Second Edition, Springer Verlag, 2010

Reference Book:

1. *Stabilization, Safety, and Security of Distributed Systems,* Rachid Guerraoui and Franck Petit,Springer, 2010
2. *Distributed Systems Security:Issues, Processes and Solutions,* Abhijit Belapurkar, Anirban Chakrabarti, Harigopal Ponnapalli, Niranjan Varadarajan, Srinivas Padmanabhuni and Srikanth Sundarrajan, Wiley publications, 2009.

Web links and Video Lectures (e-Resources):

https://www.youtube.com/watch?v=_mxufDbcK5A
https://www.youtube.com/watch?v=HvZ-05RssYw

Skill Development Activities Suggested

The students with the help of the course teacher can take up relevant technical –activities which will enhance their skill. The prepared report shall be evaluated for CIE marks.

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Able the exploit development process to identify threats.	L1
CO2	Search for vulnerabilities in closed-source applications	L2
CO3	Write their own exploits for vulnerable applications	L2
CO4	Develop the security architecture designed for any system, systems and cloud based services and mitigate it.	L2

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1		X										
CO2					X			X				X
CO3	X					X				X		
CO4			X									X

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	Po1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
3	Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.	PO3
4	Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.	PO4
5	Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations	PO5
6	The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering and business practices.	PO6
7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9
10	Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.	PO10
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.	PO11
12	Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.	PO12

ADVANCED CRYPTOGRAPHIC TECHNIQUES

Course Code	**22SFC15**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	2:0:2	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:
- Know the Basics of Encryption Techniques.
- Illustrate the Basic Concepts in Number Theory
- Define Public key encryption and Key Management and Distribution

Module-1

Classical Encryption Techniques Symmetric Cipher Model, Cryptography, Cryptanalysis and BruteForce Attack, Substitution Techniques, Caesar Cipher, Mono-alphabetic Cipher, Playfair Cipher, Hill Cipher, Poly alphabetic Cipher, One Time Pad. Block Ciphers and the data encryption standard: Traditional block Cipher structure, stream Ciphers and block Ciphers, Motivation for the Feistel Cipher structure, the Feistel Cipher, The data encryption standard, DES encryption, DES decryption, A DES example, results, the avalanche effect, the strength of DES, the use of 56-Bit Keys, the nature of the DES algorithm, timing attacks, Block cipher design principles, number of rounds, design of function F, key schedule algorithm.

Teaching-Learning Process	Chalk and talk method / PowerPoint Presentation

Module-2

Basic Concepts in Number Theory and Finite Fields :Divisibility and The Division Algorithm, The Euclidean Algorithm, Modular Arithmetic, Groups, Rings, and Fields , Finite Fields of the Form GF(p) ,Polynomial Arithmetic , Finite Fields of the Form GF(2n). Advanced Encryption Standard : Finite Field Arithmetic, AES Structure General Structure Detailed Structure, AES Transformation Functions Substitute Bytes Transformation Shift Rows Transformation Mix Columns Transformation AddRound Key Transformation ,AES Key Expansion Key Expansion Algorithm Rationale ,An AES Example Results Avalanche Effect ,AES Implementation Equivalent Inverse Cipher Implementation Aspects. Block Cipher Operation:Multiple Encryption and Triple des Double DES Triple DES with Two Keys Triple DES with Three Keys , Electronic Code Book Cipher Block Chaining Mode Cipher Feedback Mode , Output Feedback Mod

Teaching-Learning Process	Chalk and talk method / PowerPoint Presentation

Module-3

Public-Key Cryptography and RSA,The RSA algorithm, Other Public-Key Cryptosystems: Diffie-Hellman Key Exchange The Algorithm Key Exchange Protocols Man-in-the-Middle Attack ,Elgamal Cryptographic System , Elliptic Curve Arithmetic Abelian Groups Elliptic Curves over Real Numbers Elliptic Curves over Zp Elliptic Curves over GF(2m) ,Elliptic Curve Cryptography Analog of Diffie-Hellman Key Exchange Elliptic Curve Encryption/Decryption Security of Elliptic Curve Cryptography

Teaching-Learning Process	Chalk and talk method / PowerPoint Presentation

Module-4

Key Management and Distribution :Symmetric Key Distribution Using Symmetric Encryption Symmetric Key Distribution Using Asymmetric Encryption Distribution of Public Keys X.509 Certificates Public-Key Infrastructure , User Authentication Remote User-Authentication Principles Remote User-Authentication Using Symmetric Encryption Kerberos Remote User Authentication Using Asymmetric Encryption Federated Identity Management Personal Identity Verification 484	
Teaching-Learning Process	**Chalk and talk method / PowerPoint Presentation**

Module-5	
Transport-Level Security Web Security Considerations Secure Sockets Layer Transport Layer Security HTTPS Secure Shell (SSH) Wireless Security Wireless Network Threats Wireless Security Measures Mobile Device Security Security Threats Mobile Device Security Strategy Pretty Good Privacy Notation Operational Description S/MIME RFC 5322 Multipurpose Internet Mail Extensions S/MIME Functionality S/MIME Messages S/MIME Certificate Processing Enhanced Security Services	
Teaching-Learning Process	**Chalk and talk method / PowerPoint Presentation**

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Three Unit Tests each of **20 Marks**
2. Two assignments each of **20 Marks** or **one Skill Development Activity of 40 marks** to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:

1. The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
2. The question paper will have ten full questions carrying equal marks.
3. Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
4. Each full question will have a sub-question covering all the topics under a module.
5. The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:
Books

1. *Cryptography and Network Security Principles And Practice William Stallings*,Pearson Education, Fourth Edition
2. *A Course in Number Theory and Cryptology,* Neal Koblitz ,Springer, 1987
3. *Cryptography and Network Security* ,Behrouz A Forouzan, DebdeepMukhopadh yay ,Mc-GrawHill ,3rd Edition, 2015

Web links and Video Lectures (e-Resources):

https://www.youtube.com/watch?v=rA_ZmWPormM

Skill Development Activities Suggested

The students with the help of the course teacher can take up relevant technical –activities which will enhance their skill. The prepared report shall be evaluated for CIE marks.

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Understand OSI security architecture and classical encryption techniques.	L1
CO2	Understand various block cipher and stream cipher models.	L2
CO3	Describe the principles of public key cryptosystems, hash functions and digital signature.	L2
CO4	Compare various Cryptographic Techniques	L2

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1			X				X			
CO2	X							X		X
CO3					X				X	
CO4										

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	Po1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
3	Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.	PO3
4	Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.	PO4
5	Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations	PO5
6	The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering and business practices.	PO6
7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9
10	Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.	PO10

11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.	PO11
12	Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.	PO12

Common to all M tech programs in CSE board			
Research Methodology and IPR			
Course Code	**22RMI16**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	3:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:

- To introduce various technologies of conducting research.
- To choose an approptiate rsearch design for the choosen problem.
- Choose appropriate tool for the conduction of research.
- To explain the art of interpretation and the art of writing research reports.
- To explain various forms of the intellectual property, its relevance and business impact in the changing global business environment
- To discuss leading International Instruments concerning Intellectual Property Rights.

Module-1

Research Methodology: Introduction, Meaning of Research, Objectives of Research, Motivation in Research, Types of Research, Research Approaches, Significance of Research, Research Methods versus Methodology, Research and Scientific Method, Importance of Knowing How Research is Done, Research Process, Criteria of Good Research, and Problems Encountered by Researchers in India. **Defining the Research Problem:** Research Problem, Selecting the Problem, Necessity of Defining the Problem, Technique Involved in Defining a Problem, An Illustration

Teaching-Learning Process	Chalk and talk/PPT/case study

Module-2

Reviewing the literature: Place of the literature review in research, Bringing clarity and focus to your research problem, Improving research methodology, Broadening knowledge base in research area, Enabling contextual findings, How to review the literature, searching the existing literature, reviewing the selected literature, Developing a theoretical framework, Developing a conceptual framework, Writing about the literature reviewed.

Research Design: Meaning of Research Design, Need for Research Design, Features of a Good Design, Important Concepts Relating to Research Design, Different Research Designs, Basic Principles of Experimental Designs, Important Experimental Designs.

Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Module-3

Design of Sampling: Introduction, Sample Design, Sampling and Non-sampling Errors, Sample Survey versus Census Survey, Types of Sampling Designs. **Measurement and Scaling:** Qualitative and Quantitative Data, Classifications of Measurement Scales, Goodness of Measurement Scales, Sources of Error in Measurement Tools, Scaling, Scale Classification Bases, Scaling Technics, Multidimensional Scaling, Deciding the Scale. **Data Collection:** Experimental and Surveys, Collection of Primary Data, Collection of Secondary Data, Selection of Appropriate Method for Data Collection, Case Study Method.

Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Module-4

Testing of Hypotheses: Hypothesis, Basic Concepts Concerning Testing of Hypotheses, Testing of Hypothesis, Test Statistics and Critical Region, Critical Value and Decision Rule, Procedure for Hypothesis Testing, Hypothesis Testing for Mean, Proportion, Variance, for Difference of Two Mean, for Difference of Two Proportions, for Difference of Two Variances, P-Value approach, Power of Test, Limitations of the Tests of Hypothesis. **Chi-square Test:** Test of Difference of more than Two Proportions, Test of Independence of Attributes, Test of Goodness of Fit, Cautions in Using Chi Square Tests	
Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Module-5
Interpretation and Report Writing: Meaning of Interpretation, Technique of Interpretation, Precaution in Interpretation, Significance of Report Writing, Different Steps in Writing Report, Layout of the Research Report, Types of Reports, Oral Presentation, Mechanics of Writing a Research Report, Precautions for Writing Research Reports. **Intellectual Property:** The Concept, Intellectual Property System in India, Development of TRIPS Complied Regime in India, Patents Act, 1970, Trade Mark Act, 1999,The Designs Act, 2000, The Geographical Indications of Goods (Registration and Protection) Act1999, Copyright Act,1957,The Protection of Plant Varieties and Farmers' Rights Act, 2001,The Semi-Conductor Integrated Circuits Layout Design Act, 2000, Trade Secrets, Utility Models, IPR and Biodiversity, The Convention on Biological Diversity (CBD) 1992, Competing Rationales for Protection of IPRs, Leading International Instruments Concerning IPR, World Intellectual Property Organisation (WIPO),WIPO and WTO, Paris Convention for the Protection of Industrial Property, National Treatment, Right of Priority, Common Rules, Patents, Marks,   Industrial Designs, Trade Names, Indications of Source, Unfair Competition, Patent Cooperation Treaty (PCT), Advantages of PCT Filing, Berne Convention for the Protection of Literary and Artistic Works, Basic Principles, Duration of Protection, Trade Related Aspects of Intellectual Property Rights(TRIPS) Agreement, Covered under TRIPS Agreement, Features of the Agreement, Protection of Intellectual Property under TRIPS, Copyright and Related Rights, Trademarks, Geographical indications, Industrial Designs,   Patents, Patentable Subject Matter, Rights Conferred, Exceptions, Term of protection, Conditions on Patent Applicants, Process Patents, Other Use without Authorization of the Right Holder,   Layout-Designs of Integrated Circuits, Protection of Undisclosed Information, Enforcement of Intellectual Property Rights, UNSECO.

Teaching-Learning Process	Chalk and talk/PPT

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Three Unit Tests each of **20 Marks**
2. Two assignments each of **20 Marks**or**one**Skill Development Activity of 40 marks**
3. to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:

1. The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
2. The question paper will have ten full questions carrying equal marks.
3. Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
4. Each full question will have a sub-question covering all the topics under a module.
5. The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:

Text Books:

1. *Research Methodology: Methods and Techniques*, C.R. Kothari, Gaurav Garg,New Age International,4th Edition, 2018.. Douglas E Comer, "Internetworking with TCP/IP, Principles, Protocols and Architecture," PHI, 6th Edition

2. *Research Methodology a step-by-step guide for beginners.* (For the topic Reviewing the literature under module 2), RanjitKumar,SAGE Publications,3rd Edition, 2011.

Reference Books:

1. *Research Methods: the concise knowledge base,* Trochim, Atomic Dog Publishing, 2005.

2. *Conducting Research Literature Reviews: From the Internet to Paper,* Fink A, Sage Publications, 2009.

Web links and Video Lectures (e-Resources):

- https://www.youtube.com/watch?v=A7oioOJ4g0Y&list=PLVf5enqoJ-yVQ2RXUl6mCfLPf3J_JUfoc

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Conduct research independently	L2
CO2	Choose research designs, sampling designs, measurement and scaling techniques and also different methods of data collections.	L2
CO3	Statistically interpret the data and draw inferences	L2

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1		x		x								x
CO2		x	x									x
CO3				x	x							x

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	PO1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
3	Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.	PO3

4	Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.	PO4
5	Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations	PO5
6	The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering and business practices.	PO6
7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9
10	Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.	PO10
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.	PO11
12	Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.	PO12

NETWORK FORENSICS LABORATORY			
Course Code	**2SFCL17**	CIE Marks	50
Teaching Hours/Week (L:P: S)	1:2:0	SEE Marks	50
Credits	02	Exam Hours	03

Course objectives:
- Study the Different Forensic tools

Sl. NO	Experiments
1	How to Recover Deleted Files using Forensics Tools
2	Study the steps for hiding and extract any text file behind an image file/ Audio file using Command Prompt.
3	How to Extract Exchangeable image file format (EXIF) Data from Image Files using Exifreader Software
4	How to make the forensic image of the hard drive using EnCase Forensics.
5	How to Restoring the Evidence Image using EnCase Forensics
6	How to Collect Email Evidence in Victim PC
7	How to Extracting Browser Artifacts
8	How to View Last Activity of Your PC

Course outcomes (Course Skill Set):
At the end of the course the student will be able to:
- Demonstrate the how to Recover Deleted Files .
- Demonstrate Restoring the Evidence Image using EnCase Forensics.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each course. The student has to secure not less than 40% of maximum marks in the semester-end examination(SEE). In total of CIE and SEE student has to secure 50% maximum marks of the course.

Continuous Internal Evaluation (CIE):

CIE marks for the practical course is **50 Marks**.

The split-up of CIE marks for record/ journal and test are in the ratio **60:40**.

- Each experiment to be evaluated for conduction with observation sheet and record write-up. Rubrics for the evaluation of the journal/write-up for hardware/software experiments designed by the faculty who is handling the laboratory session and is made known to students at the beginning of the practical session.
- Record should contain all the specified experiments in the syllabus and each experiment write-up will be evaluated for 10 marks.
- Total marks scored by the students are scaled downed to 30 marks (60% of maximum marks).
- Weightage to be given for neatness and submission of record/write-up on time.
- Department shall conduct 02 tests for 100 marks, the first test shall be conducted after the 8th week of the semester and the second test shall be conducted after the 14th week of the semester.
- In each test, test write-up, conduction of experiment, acceptable result, and procedural knowledge will carry a weightage of 60% and the rest 40% for viva-voce.
- The suitable rubrics can be designed to evaluate each student's performance and learning ability.
- The average of 02 tests is scaled down to **20 marks** (40% of the maximum marks).

The Sum of **scaled-down** marks scored in the report write-up/journal and average marks of two tests is the total CIE marks scored by the student.

Semester End Evaluation (SEE):

SEE marks for the practical course is 50 Marks.

SEE shall be conducted jointly by the two examiners of the same institute, examiners are appointed by the University.

All laboratory experiments are to be included for practical examination.

(Rubrics) Breakup of marks and the instructions printed on the cover page of the answer script to be strictly adhered to by the examiners. **OR** based on the course requirement evaluation rubrics shall be decided jointly by examiners.

Students can pick one question (experiment) from the questions lot prepared by the internal /external examiners jointly.

Evaluation of test write-up/ conduction procedure and result/viva will be conducted jointly

by examiners.

General rubrics suggested for SEE are mentioned here, writeup-20%, Conduction procedure and result in -60%, Viva-voce 20% of maximum marks. SEE for practical shall be evaluated for 100 marks and scored marks shall be scaled down to 50 marks (however, based on course type, rubrics shall be decided by the examiners)

Change of experiment is allowed only once and 10% Marks allotted to the procedure part to be made zero.

The duration of SEE is 03 hours

PRESERVING AND RECOVERING DIGITAL EVIDENCE

Course Code	**22SFC21**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	2:0:2	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:

- Define what is digital evidence, investigation technology
- Illustrate about forensic examination of Unix system
- Explain how to apply digital evidence o network and transport layer.

Module-1
Digital evidence and computer crime: history and terminals of computer crime investigation, technology and law, the investigate process, investigate reconstruction, modus operandi, motive and technology, digital evidence in the court room.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

Module-2
Computer basics for digital investigators: applying forensic science to computers, forensic examination of windows systems, forensic examination of Unix systems, forensic examination of Macintosh systems, and forensic examination of handheld devices

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

Module-3
Networks basics for digital investigators: applying forensic science to networks, digital evidence on physical and datalink layers, digital evidence on network and transport layers, digital evidence on the internet.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

Module-4
Investigating computer intrusions, investigating cyber stalking, digital evidence as alibi.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

Module-5
Handling the digital crime scene, digital evidence examination guidelines.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Three Unit Tests each of **20 Marks**
2. Two assignments each of **20 Marks** or **one Skill Development Activity of 40 marks** to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:

1. The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
2. The question paper will have ten full questions carrying equal marks.
3. Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
4. Each full question will have a sub-question covering all the topics under a module.
5. The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:

Text Books

1. *Digital Evidence and Computer Crime Forensic science, Computers and Internet,* Eoghan Casey, Elsevier Academic Press, Second Edition.

Reference Books

1. *Digital Forensic for Network, Internet, and Cloud Computing A forensic evidence guide for moving Targets and Data*, Terrence V.Lillard, Glint P.Garrison, Craig A.Schiller, James Steele Syngress

2. *The Best Damn Cybercrime and Digital Forensics Book Period,*Jack Wiles , Anthony Reyes , Jesse Varsalone ,Syngress ,Edition 1st, 2007

Web links and Video Lectures (e-Resources):

- https://youtu.be/s01A-yqOby8

Skill Development Activities Suggested

The students with the help of the course teacher can take up relevant technical –activities which will enhance their skill. The prepared report shall be evaluated for CIE marks.

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Explain Digital evidence and computer crime and Laws(can be attained through assignment or CIE)	L3
CO2	Illustrate the Computer basics for digital investigators w.r.t Unix and Macintosh systems	L2
CO3	Illustrate the Networks basics for digital investigators	L2
CO4	Able to investigate computer intrusions and cyber stalking(can be attained through assignment or CIE)	L3
CO5	Explain the basic concepts how to handling the digital crime scene, digital evidence examination guidelines	L2

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1								X				X
CO2		X			X					X		
CO3												X
CO4	X							X				
CO5			X		X							

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	PO1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
3	Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.	PO3
4	Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.	PO4

5	Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations	PO5
6	The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering and business practices.	PO6
7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9
10	Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.	PO10
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.	PO11
12	Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.	PO12

CLOUD SECURITY AND FORENSICS

Course Code	**22SFC22**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	3:2:0	SEE Marks	50
Total Hours of Pedagogy	40 hours Theory + 10 hours Lab	Total Marks	100
Credits	04	Exam Hours	

Course objectives:
- Illustrate the basic of Cloud computing.
- Study the Cloud and infrastructure security.
- Describe Cloud Storage Forensic Framework and Dropbox analysis
- Study the Forensic analysis of Cloud storage and data

MODULE-1

Introduction to Cloud Computing: Cloud Computing (NIST Model): Introduction to Cloud Computing, History of Cloud Computing, cloud service providers. Properties, Characteristics & Disadvantages: Pros and Cons of Cloud Computing, Benefits of Cloud Computing, Cloud computing vs. Cluster computing vs. Grid computing. Role of Open Standards.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

MODULE-2

Cloud Security, Infrastructure Security, Network level security, Host level security, Application level security, Data security and Storage, Data privacy and security Issues, Jurisdictional issues raised by Data location, Identity& Access Management, Access Control, Trust, Reputation, Risk, Authentication in cloud computing, Client access in cloud, Cloud contracting Model, Commercial and business considerations, Case Study on Open Source & Commercial Clouds –Eucalyptus, Microsoft Azure, Amazon EC2.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

MODULE-3

Cloud Computing Architecture: Service Models (XaaS), Deployment Models, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS).

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

MODULE-4

Cloud Storage Forensic Framework, Evidence Source Identification and preservation in the cloud storage, Collection of Evidence from cloud storage services, Examination and analysis of collected data, Dropbox analysis: Data remnants on user machines, Evidence source identification and analysis - Collection of evidence from cloud storage services, Examination and analysis of collected data,

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

MODULE 5
Google Drive: Forensic analysis of Cloud storage and data remnants o Evidence source identification and analysis Collection of evidence from cloud storage services o Examination and analysis of collected data, Issues in cloud forensics, Case Studies.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

PRACTICAL COMPONENT OF IPCC *(May cover all / major modules)*

Sl.NO	Experiments
1	Build private cloud using open source tools.
2	Perform Case Study of sample cloud services
3	Case Study on Platform as a Service(PaaS) (Face book, Google App Engine)
4	Performing forensic analysis in a cloud environment that has fallen victim to an attack.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together

CIE for the theory component of IPCC

1. Two Tests each of **20 Marks**

2. Two assignments each of **10 Marks/One Skill Development Activity of 20 marks**
3. Total Marks of two tests and two assignments/one Skill Development Activity added will be CIE for 60 marks, marks scored will be proportionally scaled down to **30 marks**.

CIE for the practical component of IPCC

- On completion of every experiment/program in the laboratory, the students shall be evaluated and marks shall be awarded on the same day. The **15 marks** are for conducting the experiment and preparation of the laboratory record, the other **05 marks shall be for the test** conducted at the end of the semester.
- The CIE marks awarded in the case of the Practical component shall be based on the continuous evaluation of the laboratory report. Each experiment report can be evaluated for 10 marks. Marks of all experiments' write-ups are added and scaled down to 15 marks.
- The laboratory test at the end /after completion of all the experiments shall be conducted for 50

marks and scaled down to 05 marks**.**

Scaled-down marks of write-up evaluations and tests added will be CIE marks for the laboratory component of IPCC for **20 marks**.

SEE for IPCC

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (duration 03 hours)

1. The question paper will be set for 100 marks and marks scored will be scaled down proportionately to 50 marks.
2. The question paper will have ten questions. Each question is set for 20 marks.
3. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.
4. The students have to answer 5 full questions, selecting one full question from each module.

The theory portion of the IPCC shall be for both CIE and SEE, whereas the practical portion will have a CIE component only. Questions mentioned in the SEE paper shall include questions from the practical component).

- The minimum marks to be secured in CIE to appear for SEE shall be the 15 (50% of maximum marks-30) in the theory component and 10 (50% of maximum marks -20) in the practical component. The laboratory component of the IPCC shall be for CIE only. However, in SEE, the questions from the laboratory component shall be included. The maximum of 04/05 questions to be set from the practical component of IPCC, the total marks of all questions should not be more than the 20 marks.
- SEE will be conducted for 100 marks and students shall secure 40% of the maximum marks to qualify in the SEE. Marks secured will be scaled down to 50. (Student has to secure an aggregate of 50% of maximum marks of the course(CIE+SEE)

Suggested Learning Resources:
Text Books
1. *Cloud Security and Privacy, An Enterprise Perspective on Risks and Compliance Tim Mather*, Subra Kumaraswamy, Shahed Latif ,Oreilly Media 2009.
2. *Securing the Cloud, Cloud Computer Security Techniques and Tactics Vic (J.R.)* ,Winkler Syngress 2011

Web links and Video Lectures (e-Resources):
https://www.youtube.com/watch?v=EEdjTRS_jpQ
https://www.youtube.com/watch?v=7I-dcPi4NNE

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Explain the growth of Cloud computing, architecture and different modules of implementation.	L2
CO2	Illustrate the different types of cloud solutions among IaaS, PaaS, SaaS.	L2
CO3	Explain Access the security implementation flow, actions and responsibilities of stake holders.	L2
CO4	Generalize the Data Centre operations, encryption methods and deployment details.	L2
CO5	Provide recommendations for using and managing the customer's identity and choose the type of virtualization to be used.	L2

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	X								X			
CO2			X					X				
CO3									X			X
CO4												X
CO5	X											X

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	PO1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
3	Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.	PO3
4	Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.	PO4
5	Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations	PO5
6	The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering and business practices.	PO6

7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9
10	Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.	PO10
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.	PO11
12	Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.	PO12

SECURED PROGRAMMING			
Course Code	**22SFC231**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	2:0:2	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:

- Study the Pre pocessor and Declaration of Variables.
- Define the Expression, Integer and floating point number representation.
- Demonstrate the Arrays, Strings and memory management concepts.
- Explain Signal and Error handling concepts.

Module-1

Pre-processor, Declarations and Initializations: universal character name through concatenation, arguments to unsafe macros, invocations of function-like macros. Declare objects with appropriate storage durations, Identifier declaration with conflict linkage classifications, Using correct syntax for declaring flexible array member, Avoiding information leakage in structure padding, Incompatible declarations of same function or object

Teaching-Learning Process	Chalk and Talk method /PPT/

Module-2

Expressions and Integer : Dependence on evaluation order for side effects: Reading uninitialized memory and dereferencing null pointers, Modifying objects with temporary lifetime, Accessing variable through (pointer) incompatible type, Modifying constant objects and comparing padding data. Wrapping of unsigned integers, Integer conversions and misrepresented data, Integer overflow and divide by zero errors, Shifting of negative numbers, Using correct integer precisions, Pointer conversion to integer and vice versa.

Teaching-Learning Process	Chalk and Talk method /PPT/ Web contents

Module-3

Floating Point, Arrays and Strings: Floating point values for counters: Domain and range errors in math functions, Floating point conversions and preserving precision. Out of bounds subscripts and valid length arrays, Comparing array pointers, Pointer arithmetic for non-array object, scaled integer.Modifying string literals, Space allocation for strings (Null terminator), Casting large integers as unsigned chars, Narrow and wide character strings and functions.

Teaching-Learning Process	Chalk and Talk method /PPT/ Web contents

Module-4

Memory Management , I/O:Accessing freed memory: Freeing dynamically allocated memory, Computing memory allocation for an object, Copying structures containing flexible array members, Modifying object alignment by using realloc. User input and format strings, Opening an pre-opened file, Performing device operations appropriate for files, Dealing with EOF, WEOF, Copying FILE object, Careful use of fgets, fgetws, getc, putc, putwc. Use of fsetops and fgetops, Accessing closed files.

Teaching-Learning	Chalk and Talk method /PPT/ Web contents

Module-5
Environment ,Signals and Error Handing: environment pointer following an operation, system(),pointers returned by certain functions.Using asynchronous safe functions and signal handlers: Shared objects and signal handlers, Using signal() within interruptible signal handlers, Returning computation exception signal handler. Using errno: check and set, Depending upon indeterminate values of errno, Handling standard library errors.

Teaching-Learning Process	Chalk and Talk method /PPT/ Web contents

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Three Unit Tests each of **20 Marks**
2. Two assignments each of **20 Marks** or **one Skill Development Activity of 40 marks**
3. to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:

1. The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
2. The question paper will have ten full questions carrying equal marks.
3. Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
4. Each full question will have a sub-question covering all the topics under a module.
5. The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:
Text Books

1. *The CERT ® C Coding Standard: 98 Rules for Developing Safe, Reliable, and Secure Systems,* Robert C. Seacord ,Addison ,Wesley Professional ,Second Edition ,2014

 Reference Books

1. *Secure Programming for Linux and Unix HowTo David Wheeler Linux Documentation project* 2004.

2. *Secure Programming Cookbook for C and C++*, JohnViega, Matt Messier ,O'Reilly Media, 2003

Web links and Video Lectures (e-Resources):

- https://youtu.be/s01A-yqOby8

Skill Development Activities Suggested

The students with the help of the course teacher can take up relevant technical –activities which will enhance their skill. The prepared report shall be evaluated for CIE marks.

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	How to respond to security alerts which identifies software issues	L2
CO2	Identify possible security programming errors	L2
CO3	Define methodology for security testing and use appropriate tools in its implementation	L2
CO4	Apply new security-enhanced programming models and tools(can be attained through assignment or CIE)	L3

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												X
CO2					X					X		
CO3				X			X					X
CO4			X									X

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	PO1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
3	Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.	PO3
4	Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.	PO4
5	Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations	PO5
6	The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering and business practices.	PO6

7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9
10	Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.	PO10
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.	PO11
12	Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.	PO12

FILE SYSTEM FORENSIC ANALYSIS			
Course Code	**22SFC232**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	2:0:2	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:

- Explore Volume analysis.
- Illustrate the File system analysis.
- Define NTFS Concepts and Ext2 & Ext3.
- Illustrate the working of UFS2 & UFS2.

Module-1
Computer foundations: Data organizations, booting process, Hard disk technology, Hard disk data acquisition- introduction, reading the source data, writing the output data. Volume Analysis: Introduction, Background, Analysis Basics, Summary. PC-based Partitions: DOS Partitions, Analysis Considerations, Apple Partitions, Removable Media. Server-based Partitions: BSD Partitions, Sun Solaris Slices, GPT Partitions

Teaching-Learning Process	Chalk and Talk method /PPT

Module-2
File System Analysis: What Is a File System?, File System Category, Content Category, Metadata Category, File Name Category, Application Category, Application-level Search Techniques, Specific File Systems FAT Concepts and Analysis: Introduction, File System Category, Content Category, Metadata Category, File Name Category, The Big Picture.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

Module-3
NTFS Concepts: Introduction, Everything is a File, MFT Concepts, MFT Entry Attribute Concepts, Other Attribute Concepts, Indexes, Analysis Tools. NTFS Analysis: File System Category, Content Category, Metadata Category, File Name Category, Application Category, The Big Picture. NTFS Data Structures: Basic Concepts, Standard File Attributes, Index Attributes and Data Structures.

Teaching-Learning Process	Chalk and Talk method /PPT

Module-4
Ext2 and Ext3 Concepts and Analysis: Introduction, File System Category, Content Category, Metadata Category, File Name Category, Application Category. The Big Picture. Ext2 and Ext3 Data Structures: Superblock, Group Descriptor Tables, Block Bitmap, Inodes, Extended Attributes.

Teaching-Learning Process	Chalk and Talk method /PPT

Module-5
UFS1 and UFS2 Concepts and Analysis: Introduction, File System Category, Content Category, Metadata Category, File Name Category, The Big Picture. UFS1 and UFS2 Data Structures: UFS1 Superblock, UFS2 Superblock, Cylinder Group Summary, UFS1 Group Descriptor, UFS2 Group Descriptor.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Three Unit Tests each of **20 Marks**
2. Two assignments each of **20 Marks** or **one Skill Development Activity of 40 marks** to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:

1. The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
2. The question paper will have ten full questions carrying equal marks.
3. Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
4. Each full question will have a sub-question covering all the topics under a module.
5. The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:

Text Books

1. *File System Forensic ,* Brian Carrier, Pearson Education ,2005
2. *Digital Evidence and Computer Crime,* Casey Eoghan ,Academic Press, Edition 3, 2011.

Reference Books

1. Introduction to Linux A Hands-On Guide, MachteltGarrels, Fultus CorporationPublisher, Third Edition 2010.

2. Computer Forensics, Warren and Jay Heiser, Kruse, Addison Wesley, 2002.

3. Guide to Computer Forensics and Investigations, Bill Nelson, Amelia Phillips, Frank Enfinger, Chris Steuart, Thomson Course Technology, 2004

4. Forensic Discovery, Dan Farmer & WietseVenema, Addison Wesley, 2005

Web links and Video Lectures (e-Resources):

* https://www.youtube.com/watch?v=2ESqwX3qb94

Skill Development Activities Suggested

The students with the help of the course teacher can take up relevant technical –activities which will enhance their skill. The prepared report shall be evaluated for CIE marks.

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Explain the foundation of digital investigation and methods of data analysis	L2
CO2	Illustrate the role of computer forensics in the business and private world	L2
CO3	Identify some of the current techniques and tools for forensic examinations	L2
CO4	Familiarize the NTFS file systems	L2

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1				X								X
CO2		X			x				X			
CO3	X											X

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	PO1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
3	Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.	PO3
4	Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.	PO4
5	Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations	PO5
6	The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering and business practices.	PO6
7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7

8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9
10	Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.	PO10
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.	PO11
12	Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.	PO12

LAWS RELATED TO CYBER SECURITY

Course Code	**22SFC233**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	2:0:2	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:
- Explain a Critical Understanding Cyber Law
- Develop Competencies For Dealing With Frauds And Deceptions
- Explore Other Cyber Crimes For Example, Child Pornography Etc. That Are Taking Place Via The Internet.

Module-1

Introduction to Cyber Law Evolution of Computer Technology : Emergence of Cyber space. Cyber Jurisprudence, Jurisprudence and law, Doctrinal approach, Consensual approach, Real Approach, Cyber Ethics, Cyber Jurisdiction, Hierarchy of courts, Civil and criminal jurisdictions, Cyberspace-Web space, Web hosting and web Development agreement, Legal and Technological Significance of domain Names, Internet as a tool for global access.

Teaching-Learning Process	**Chalk and Talk method /PPT/ Case study**

Module-2

Information technology Act : Overview of IT Act, 2000, Amendments and Limitations of IT Act, Digital Signatures, Cryptographic Algorithm, Public Cryptography, Private Cryptography, Electronic Governance, Legal Recognition of Electronic Records, Legal Recognition of Digital Signature Certifying Authorities, Cyber Crime and Offences, Network Service Providers Liability, Cyber Regulations Appellate Tribunal, Penalties and Adjudication.

Teaching-Learning Process	**Chalk and Talk method /PPT/ Case study/Web contents**

Module-3

Cyber law and related Legislation : Patent Law, Trademark Law, Copyright, Software – Copyright or Patented, Domain Names and Copyright disputes, Electronic Data Base and its Protection, IT Act and Civil Procedure Code, IT Act and Criminal Procedural Code, Relevant Sections of Indian Evidence Act, Relevant Sections of Bankers Book Evidence Act, Relevant Sections of Indian Penal Code, Relevant Sections of Reserve Bank of India Act, Law Relating To Employees And Internet, Alternative Dispute Resolution , Online Dispute Resolution (ODR).

Teaching-Learning Process	**Chalk and Talk method /PPT/ Case study/Web contents**

Module-4

Electronic Business and legal issues: Evolution and development in Ecommerce, paper vs paper less contracts E-Commerce models- B2B, B2C,E security. Application area: Business, taxation, electronic payments, supply chain, EDI, E-markets, Emerging Trends.

Teaching-Learning Process	**Chalk and Talk method /PPT/ Case study/Web contents**

Module-5

Case Study On Cyber Crimes: Harassment Via E-Mails, Email Spoofing (Online A Method Of Sending E-Mail Using A False Name Or E-Mail Address To Make It Appear That The E-Mail Comes From Somebody Other Than The True Sender, Cyber Pornography (Exm.MMS),Cyber-Stalking.

Teaching-Learning Process	**Chalk and Talk method /PPT/ Case study/Web contents**

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Three Unit Tests each of 20 Marks
2. Two assignments each of 20 Marks or one Skill Development Activity of 40 marks
3. to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be scaled down to 50 marks

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:

1. The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
2. The question paper will have ten full questions carrying equal marks.
3. Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
4. Each full question will have a sub-question covering all the topics under a module.
5. The students will have to answer five full questions, selecting one full question from each module

.

Suggested Learning Resources:

Text Books

1. *Cyber Laws: Intellectual property & E Commerce, Security* ,K.Kumar, Dominant Publisher,1st Edition, 2011.

2. Rodney D. Ryder, " Guide To Cyber Laws", Second Edition, Wadhwa And Company, New Delhi, 2007.

  Reference Books

1. Information Security policy &implementation Issues, NIIT, PHI

2. *Handbook Of Cyber Laws*, Vakul Sharma, Macmillan India Ltd, 2nd Edition,PHI,2003.

3. *Cyber Laws*, Justice Yatindra Singh Universal Law Publishing, 1 st Edition,New Delhi, 2003.

4. *Dimensions Of Cyber Crime*, Sharma, S.R., Annual Publications Pvt. Ltd., 1st Edition, 2004.

5. *Cyber Crimes And Legal Issues*, Augastine, Paul TCrecent Publishing Corporation, 2007.

Web links and Video Lectures (e-Resources):

- https://www.youtube.com/watch?v=F7mH5vz1qEI
- https://www.youtube.com/watch?v=BvWvFAS1iP0

Skill Development Activities Suggested

The students with the help of the course teacher can take up relevant technical –activities which will enhance their skill. The prepared report shall be evaluated for CIE marks.

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Explain the social and intellectual property issues emerging from cyberspace. (can be attained through assignment or CIE)	L3
CO2	Interpreat the legal and policy developments in various countries to regulate cyberspace;	L2
CO3	Describe the relationship between commerce and cyberspace.	L2
CO4	Analyze learners in depth knowledge of information technology act and legal frame work of right to privacy, data security and data protection. (can be attained through assignment or CIE)	L3

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1								X				X
CO2					X					X		
CO3												X
CO4	X							X				
CO5			X			X						

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	PO1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
3	Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.	PO3
4	Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.	PO4
5	Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations	PO5
6	The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering and business practices.	PO6

7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9
10	Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.	PO10
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.	PO11
12	Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.	PO12

BIOMETRIC SECURITY

Course Code	**22SFC234**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	2:0:2	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:

- Explain Physiological Biometric Technologies and Iris scan.
- Able to demostrate Handprint Biometrics, DNA Biometrics
- Define Multi biometrics and multi factor biometrics

Module-1
Biometrics: Introduction, benefits of biometrics over traditional authentication systems, benefits of biometrics in identification systems, selecting a biometric for a system, Applications, Key biometric terms and processes, biometric matching methods, Accuracy inbiometric systems.

Teaching-Learning Process	**Chalk and Talk method /PPT/ Case study**

Module-2
Physiological Biometric Technologies: Fingerprints: Technical description, characteristics, Competing technologies, strengths, weaknesses, deployment. Facial scan: Technical description, characteristics, weaknesses, deployment. Iris scan: Technical description, characteristics, strengths, weaknesses, deployment. Retina vascular pattern: Technical description, characteristics, strengths, weaknesses, deployment. Hand scan: Technical description, characteristics, strengths, weaknesses, deployment , DNA biometrics.

Teaching-Learning Process	**Chalk and Talk method /PPT/ Case study**

Module-3
Behavioural Biometric Technologies: Handprint Biometrics, DNA Biometrics, signature and handwriting technology, Technical description, classification, keyboard / keystroke Dynamics, Voice, data acquisition, feature extraction, characteristics, strengths, weaknesses deployment.

Teaching-Learning Process	**Chalk and Talk method /PPT/ Case study**

Module-4
Multi biometrics: Multi biometrics and multi factor biometrics, two-factor authentication with passwords, tickets and tokens, executive decision, implementation plan.

Teaching-Learning Process	**Chalk and Talk method /PPT/ Case study**

Module-5
Case studies on Physiological, Behavioural and multifactor biometrics in identification systems.

Teaching-Learning Process	**Chalk and Talk method /PPT/ Case study**

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Three Unit Tests each of **20 Marks**
2. Two assignments each of **20 Marks** or **one Skill Development Activity of 40 marks** to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:

1. The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
2. The question paper will have ten full questions carrying equal marks.
3. Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
4. Each full question will have a sub-question covering all the topics under a module.
5. The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:

Text Books

1. Biometrics –Identity verification in a networked World, Samir Nanavathi, Michel Thieme, and Raj Nanavathi ,Wiley Eastern, 2002

 Reference Books

1. *Biometrics for Network Security* ,John Berger Prentice Hall 2004

2. *Implementing Biometric Security* ,John Chirillo and Scott Blaul ,Wiley, Eastern Publications 2005

Web links and Video Lectures (e-Resources):

- https://www.digimat.in/nptel/courses/video/106104119/L01.html
- http://www.digimat.in/nptel/courses/video/106104119/L07.html
-

Skill Development Activities Suggested

The students with the help of the course teacher can take up relevant technical –activities which will enhance their skill. The prepared report shall be evaluated for CIE marks.

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Being able to Model traditional and biometric systems	L2
CO2	Analyze different algorithms of biometric systems(can be attained through assignment or CIE)	L3
CO3	Compare strengths and weaknesses of different biometric systems. (can be attained through assignment or CIE)	L3
CO4	Demonstrate different biometric system.	L2
CO5	Implement multimodal biometric systems	L2

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1			X	X								X
CO2		X							X			
CO3			X									X
CO4									X			
CO5									X			X

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	PO1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
3	Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.	PO3
4	Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.	PO4
5	Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations	PO5
6	The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering and business practices.	PO6

7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9
10	Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.	PO10
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.	PO11
12	Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.	PO12

INFORMATION SECURITY POLICIES IN INDUSTRY				
Course Code	**22SFC235**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	2:0:2	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:
- Explain the content, need, and responsibilities of information security policies.
- Explain the standards, guidelines, Procedures, and key roles of the organization.
- Able to write policy document for securing network connection and interfaces.
- Explain the threats to the stored data or data in transit and able to write policy document.
- Able to write, monitor, and review policy document.

Module-1
Introduction to Information Security Policies: About Policies, why Policies are Important, When policies should be developed, How Policy should be developed, Policy needs, Identify what and from whom it is being protected, Data security consideration, Backups, Archival storage and disposal of data, Intellectual Property rights and Policies, Incident Response and Forensics, Management Responsibilities, Role of Information Security Department, Security Management and Law Enforcement, Security awareness training and support.

Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Module-2
Policy Definitions, Standards, Guidelines, Procedures with examples, Policy Key elements, Policy format and Basic Policy Components, Policy content considerations, Program Policy Examples, Business Goal Vs Security Goals, Computer Security Objectives, Mission statement Format, Examples, Key roles in Organization, Business Objectives, Standards: International Standards.

Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Module-3
Writing The Security Policies: Computer location and Facility construction, Contingency Planning, Periodic System and Network Configuration Audits, Authentication and Network Security, Addressing and Architecture, Access Control, Login Security, Passwords, User Interface, Telecommuting and Remote Access, Internet Security Policies, Administrative and User Responsibilities, WWW Policies, Application Responsibilities, E-mail Security Policies.

Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Module-4
Establishing Type of Viruses Protection: Rules for handling Third Party Software, User Involvement with Viruses, Legal Issues, Managing Encryption and Encrypted data, Key Generation considerations and Management, Software Development policies, Processes Testing and Documentation, Revision control and Configuration management, Third Party Development, Intellectual Property Issues.

Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Module-5
Maintaining the Policies: Writing the AUP, User Login Responsibilities, Organization's responsibilities and Disclosures, Compliance and Enforcement, Testing and Effectiveness of Policies, Publishing and Notification Requirements of the Policies, Monitoring, Controls and Remedies, Administrator Responsibility, Login Considerations, Reporting of security Problems, Policy Review Process, The Review Committee, Sample Corporate Policies, Sample Security Policies.

Teaching-	Chalk and talk/PPT/case study/web content

Process	

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Three Unit Tests each of **20 Marks**
2. Two assignments each of **20 Marks** or **one Skill Development Activity of 40 marks** to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:

1. The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
2. The question paper will have ten full questions carrying equal marks.
3. Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
4. Each full question will have a sub-question covering all the topics under a module.
5. The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:

Text Books

1. *Writing Information Security Policies.* Scott Barman. Sams Publishing. 2002.

2. *Information Policies Procedures and Standards.* Thomas.R.Peltier. Thomas.R.Peltier. CRC Press. 2004.

Refence Books:

1. *Information Security Fundamentals.* Thomas R Peltier, Justin Peltier, John Backley. CRC Press,2005.

2. *Information Security Management Handbook.* Harold F. Tipton and Micki Krause. Auerbach publications. 5th Edition, 2005.

Web links and Video Lectures (e-Resources):

- https://www.mygreatlearning.com/academy/learn-for-free/courses/introduction-to-cyber-security
- This free course will introduce you to the world of cyber security. Learn about different forms of cyber attacks, cryptography, and how to design a security system, in this free online course on introduction to cyber security.

Skill Development Activities Suggested

The students with the help of the course teacher can take up relevant technical –activities which will enhance their skill. The prepared report shall be evaluated for CIE marks.

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Able to write policy document for securing network connection and interfaces.	L2
CO2	Able to explain the threats to the stored data or data in transit and able to write policy document.	L2
CO3	Able to write, monitor, and review policy document.	L2

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1		x		x						x		
CO2	x			x								
CO3		x								x		

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	PO1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
3	Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.	PO3
4	Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.	PO4
5	Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations	PO5
6	The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering and business practices.	PO6
7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9

10	Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.	PO10
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.	PO11
12	Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.	PO12

TRUST MANAGEMENT IN E-COMMERCE

Course Code	**22SFC241**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	2:0:2	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:

- Explain the E-Commerce and business models
- Define Security metrics in E-Commerce
- Describe the Inter-organizational trust in E-Commerce

Module-1

Introduction to E-Commerce: Network and E-Commerce, Types of E-Commerce. Ecommerce Business Models: B2C, B2B, C2C, P2P and M-commerce business models. Ecommerce Payment systems: Types of payment system, Credit card E-Commerce transactions, B2C E-Commerce Digital payment systems, B2B payment system.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study

Module-2

Security and Encryption: E-Commerce Security Environment, Security threats in Ecommerce environment, Policies, Procedures and Laws

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study

Module-3

Inter-organizational trust in E-Commerce: Need, Trading partner trust, Perceived benefits and risks of ECommerce, Technology trust mechanism in E-Commerce, Perspectives of organizational, economic and political theories of inter-organizational trust, Conceptual model of inter-organizational trust in ECommerce participation.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study

Module-4

Introduction to trusted computing platform: Overview, Usage Scenarios, Key components of trusted platform, Trust mechanisms in a trusted platform.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study

Module-5

Trusted platforms for organizations and individuals: Trust models and the E-Commerce domain.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case Study

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Three Unit Tests each of **20 Marks**
2. Two assignments each of **20 Marks** or **one Skill Development Activity of 40 marks**
3. to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:

1. The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
2. The question paper will have ten full questions carrying equal marks.
3. Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
4. Each full question will have a sub-question covering all the topics under a module.
5. The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:

Text Books

Study Guide to E-Commerce Business Technology Society, Kenneth C. Laudon and Carol GuercioTrave ,Pearson Education ,2005

Inter-Organizational Trust for Business-to-Business Ecommerce, Pauline Ratnasingam, IRM Press, 2005

 Reference Books

Trusted Computing Platforms: TCPA Technology in Contex,t Siani Pearson, et al Prentice Hall PTR ,2002

Web links and Video Lectures (e-Resources):

- https://www.digimat.in/nptel/courses/video/110105076/L01.html
- http://www.digimat.in/nptel/courses/video/110105083/L37.html
-

Skill Development Activities Suggested

The students with the help of the course teacher can take up relevant technical –activities which will enhance their skill. The prepared report shall be evaluated for CIE marks.

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Explain the types of E-Commerce, E-Commerce business models and E-commerce payment systems.	L2
CO2	Illustrate the Policies, Procedures and Laws and Security threats in E-Commerce environment.	L2
CO3	Analysis and explain the issues, risks and challenges in inter-organisational trust in E-Commerce(can be attained through assignment or CIE)	L3
CO4	Explain the Key components and Trust mechanisms of trusted computing platform. (can be attained through assignment or CIE)	L3
CO5	Describe the Trusted platforms for organizations and individuals(can be attained through assignment or CIE)	L3

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	X							X			X	
CO2								X			X	
CO3	X											
CO4	X							X			X	
CO5	X							X				

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	PO1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
3	Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.	PO3

4	Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.	PO4
5	Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations	PO5
6	The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering and business practices.	PO6
7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9
10	Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.	PO10
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.	PO11
12	Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.	PO12

BLOCKCHAIN TECHNOLOGY			
Course Code	**22SFC242**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	2:0:2	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:
- To explore the driving force behind the cryptocurrency Bitcoin. Along with the Decentralization,

Module-1
Blockchain 101: Distributed systems, History of blockchain, Introduction to blockchain, Types of blockchain, CAP theorem and blockchain, Benefits and limitations of blockchain.

Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Module-2
Decentralization and Cryptography: Decentralization using blockchain, Methods of decentralization, Routes to decentralization, Decentralized organizations. Cryptography and Technical Foundations: Cryptographic primitives, Asymmetric cryptography, Public and private keys

Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Module-3
Bitcoin and Alternative Coins A: Bitcoin, Transactions, Blockchain, Bitcoin payments B: Alternative Coins, Theoretical foundations, Bitcoin limitations, Namecoin, Litecoin, Primecoin, Zcash

Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Module-4
Smart Contracts and Ethereum 101: Smart Contracts: Definition, Ricardian contracts. Ethereum 101:Introduction, Ethereum blockchain, Elements of the Ethereum blockchain, Precompiled contracts.

Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Module-5
Alternative Blockchains: Blockchains Blockchain-Outside of Currencies: Internet of Things, Government, Health, Finance, Media

Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Three Unit Tests each of **20 Marks**
2. Two assignments each of **20 Marks**or**one**Skill Development Activity of 40 marks** to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:

1. The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
2. The question paper will have ten full questions carrying equal marks.
3. Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
4. Each full question will have a sub-question covering all the topics under a module.
5. The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:

Text Books:

1. *Bitcoin and Cryptocurrency Technologies,* Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, Princeton University, 2016

Reference Books:

1. *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, Daniel Drescher, Apress, First Edition, 2017

2. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies,* Andreas M. Antonopoulos, O'Reilly Media, First Edition, 2014

Web links and Video Lectures (e-Resources):

*   https://nptel.ac.in/courses/106105184
*   https://ocw.mit.edu/courses/15-s12-blockchain-and-money-fall-2018/video_galleries/video-lectures/

Skill Development Activities Suggested

The students with the help of the course teacher can take up relevant technical –activities which will enhance their skill. The prepared report shall be evaluated for CIE marks.

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Interpret the types, benefits and limitation of blockchain.	L1
CO2	Explore the blockchain decentralization and cryptography concepts.	L2
CO3	Enumerate the Bitcoin features and its alternative options.	L1

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1		x		x			x					
CO2	x			x								
CO3		x								x		

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	PO1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
3	Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.	PO3
4	Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.	PO4
5	Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations	PO5
6	The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering and business practices.	PO6
7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9
10	Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.	PO10
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.	PO11
12	Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.	PO12

Course Code	**22SFC243**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	2:0:2	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:
- Study the Learning and decision tree concepts.
- Define neural network and genetic algorithms
- Demonstrate Different learning algorithms

Module-1

INTRODUCTION, CONCEPT LEARNING and methodology ,DECISION TREES Learning Problems – Designing Learning systems, Perspectives and Issues – Concept Learning – Version Spaces and Candidate Elimination Algorithm – Inductive bias – Decision Tree learning – Representation – Algorithm – Heuristic Space Search.

Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Module-2

NEURAL NETWORKS AND GENETIC ALGORITHMS: Neural Network Representation – Problems – Perceptrons – Multilayer Networks and Back Propagation Algorithms – Advanced Topics – Genetic Algorithms – Hypothesis Space Search – Genetic Programming – Models of Evolution and Learning.

Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Module-3

BAYESIAN AND COMPUTATIONAL LEARNINGL Bayes Theorem – Concept Learning – Maximum Likelihood – Minimum Description Length Principle – Bayes Optimal Classifier – Gibbs Algorithm – Naïve Bayes Classifier– Bayesian Belief Network – EM Algorithm – Probably Learning – Sample Complexity for Finite and Infinite Hypothesis Spaces – Mistake Bound Model

Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Module-4

INSTANT BASED LEARNING AND LEARNING SET OF RULES: K- Nearest Neighbour Learning – Locally Weighted Regression – Radial Basis Functions –Case-Based Reasoning – Sequential Covering Algorithms – Learning Rule Sets – Learning First Order Rules – Learning Sets of First Order Rules – Induction as Inverted Deduction – Inverting Resolution

Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Module-5

ANALYTICAL LEARNING AND REINFORCED LEARNING: Perfect Domain Theories – Explanation Based Learning – Inductive-Analytical Approaches - FOCL Algorithm – Reinforcement Learning – Task – Q-Learning – Temporal Difference Learning

Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Three Unit Tests each of **20 Marks**
2. Two assignments each of **20 Marks** or **one** **Skill Development Activity of 40 marks** to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:

1. The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
2. The question paper will have ten full questions carrying equal marks.
3. Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
4. Each full question will have a sub-question covering all the topics under a module.
5. The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:

Text Books:

1. *Machine Learning,* Tom M. Mitchell, McGraw-Hill ,2013

Reference Books:

1. *Introduction to Machine Learning*, EthemAlpaydin PHI Learning Pvt. Ltd 2 nd Ed., 2013

2. *The Elements of Statistical Learning*, T. Hastie, R. Tibshirani, J. H. Friedman Springer 1st edition, 2001

Web links and Video Lectures (e-Resources):

https://youtu.be/r4sgKrRL2Ys

Skill Development Activities Suggested

The students with the help of the course teacher can take up relevant technical –activities which will enhance their skill. The prepared report shall be evaluated for CIE marks.

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Choose the learning techniques with this basic knowledge	L2
CO2	Apply effectively neural networks and genetic algorithms for appropriate applications(can be attained through assignment or CIE)	L3
CO3	Apply Bayesian techniques and derive effectively learning rules(can be attained through assignment or CIE)	L3
CO4	Choose and differentiate reinforcement and analytical learning techniques	L2

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1		x		x			x					
CO2	x			x								
CO3		x								x		

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	PO1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
3	Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.	PO3
4	Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.	PO4
5	Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations	PO5
6	The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering and business practices.	PO6
7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9
10	Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.	PO10
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.	PO11
12	Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.	PO12

WEB APPLICATION AND PENETRATION TESTING			
Course Code	**22SFC244**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	2:0:2	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:
- To build an end-to-end threat model landscape for web application security.
- To learn both web application vulnerabilities and web intrusion testing.
- To identify the network vulnerabilities with a web application infrastructure.

Module-1	
Building a Vulnerable Web Application Lab: Downloading Mutillidae, Installing Mutillidae on Windows, Downloading and installing XAMPP, Mutillidae installation, Installing Mutillidae on Linux, Downloading and installing XAMPP, Mutillidae installation, Using Mutillidae, User registration, Showing hints and setting security levels, Application reset. **Kali Linux Installation:** Introducing Kali Linux, Installing Kali Linux from scratch, Installing Kali on VMware, Installing Kali on VirtualBox, Bridged versus NAT versus Internal Network, Updating Kali Linux	
Teaching-Learning Process	Chalk and Talk/PPT /web resource: https://www.youtube.com/watch?v=GmWQ1VIjd2U&list=PLHUKi1UlEgOJLPSFZaFKMoexpM6qhOb4Q

Module-2	
Delving Deep into the Usage of Kali Linux: The Kali filesystem structure, Handling applications and packages, The Advanced Packaging Tool, Debian's package management system, Using dpkg commands, Handling the filesystem in Kali, File compression commands, Security management, Secure shell protocol, Configuring network services in Kali, Setting a static IP on Kali, Checking active connections in Kali, Process management commands, Htop utility, Popular commands for process management, System info commands	
Teaching-Learning Process	Chalk and Talk/PPT /web resource: https://www.youtube.com/watch?v=V7xOY5MhnQ0

Module-3	
Understanding Web Application Vulnerabilities: File Inclusion, Local File Inclusion, Remote File Inclusion, Cross-Site Scripting, Reflected XSS, Stored XSS, Cross-Site Request Forgery, Step 01 – victim, Step 02 – attacker, Results, SQL Injection, Authentication bypass, Extracting the data from the database, Error-based SQLi enumeration, Blind SQLi, Command Injection, Application Security Pre-Engagement: Introduction, The first meeting, The day of the meeting with the client, Non-Disclosure Agreement, Kick-off meeting, Time and cost estimation, Statement of work, Penetration Test Agreement, External factors,	
Teaching-Learning Process	Chalk and Talk/PPT/Assignment

Module-4	

	Network Penetration Testing: Passive information gathering – reconnaissance – OSINT, Web search engines, Google Hacking Database – Google dorks, Online tools, Kali Linux tools, WHOIS lookup, Domain name system – DNS enumeration, Gathering email addresses, Active information gathering – services enumeration, Identifying live hosts, Identifying open ports/services, Service probing and enumeration, Vulnerability assessment, OpenVas, Exploitation, Finding exploits, Listener setup, Generating a shell payload using msfvenom, Custom shells, Privilege escalation, File transfers,Using PowerShell, Using VBScript, Administrator or root, Web Intrusion Tests, Web Intrusion Test workflow, Identifying hidden contents, Common web page checklist, Special pages checklist, Reporting, Common Vulnerability Scoring System – CVSS, First case – SQLi, Second case – Reflected XSS, Report template.
Teaching-Learning Process	Chalk and Talk/PPT /web resource: https://www.youtube.com/watch?v=CktYFft7K8Q

Module-5	
	Pentest Automation Using Python: Python IDE, Downloading and installing PyCharm, PyCharm quick overview, Penetration testing automation, Automate.py in action, Utility functions, Service enumeration, DTO service class, The scanner core, Nmap Cheat Sheet, Target specification, Host discovery, Scan types and service versions, Port specification and scan order, Script scan, Timing and performance, Firewall/IDS evasion and spoofing, Output, Metasploit Cheat Sheet, Metasploit framework, Using the database, More database-related commands, Getting around, Using modules, Miscellaneous, Msfvenom, Listener scripting, Meterpreter, Netcat Cheat Sheet, Netcat command flags, Practical examples.
Teaching-Learning Process	Chalk and Talk/PPT /web resource: https://www.youtube.com/watch?v=4t4kBkMsDbQ

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Three Unit Tests each of **20 Marks**
2. Two assignments each of **20 Marks** or **one Skill Development Activity of 40 marks**
   to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.**

Semester End Examination:

1. The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
2. The question paper will have ten full questions carrying equal marks.
3. Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
4. Each full question will have a sub-question covering all the topics under a module.
5. The students will have to answer five full questions, selecting one full question from each

Suggested Learning Resources:

Text Book:

　1. Gus Khawaja, Practical Web Penetration Testing, O'Reilly Packt Publishing, 2018.

Reference Book:

　2. Christian Martorella, Learning Python Web Penetration Testing: Automate web penetration testing activities using Python Paperback, 2018.

Web links and Video Lectures (e-Resources):

- https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiziqqg9rH6AhWm-TgGHTiMDEcQwqsBegQIKxAB&url=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DX4eRbHgRawI&usg=AOvVaw0JZABUg_IAdGJY7L3DVuHu
- extension://elhekieabhbkpmcefcoobjddigjcaadp/https://dsxte2q2nyjxs.cloudfront.net/Syllabus_WAPTv3.pdf
- https://www.youtube.com/watch?v=2_lswM1S264
- https://www.youtube.com/watch?v=CktYFft7K8Q

Skill Development Activities Suggested

- Use Nmap, Metasploit, and more tools for network infrastructure tests
- Practice using all web application hacking tools for intrusion tests using Kali Linux

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Examine the web application hacking tools for intrusion tests using Kali Linux.	L1
CO2	Analyze a web application using application threat modelling.	L4
CO3	Experiment with network infrastructure tests and penetration testing functions for maximum efficiency using Python.	L3

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	x											
CO2			x									
CO3				x								

Program Outcome of this course		
Sl. No.	**Description**	**POs**
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	PO1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
3	Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.	PO3
4	Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.	PO4
5	Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations	PO5
6	The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering and business practices.	PO6
7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9
10	Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.	PO10
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.	PO11
12	Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.	PO12

OPERATING SYSTEM SECURITY			
Course Code	**22SFC245**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	2:0:2	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:
- Gain the knowledge of fundamental concepts and mechanisms for enforcing security in OS.
- Learn how to build a secure OS by exploring the early work in OS.

Module-1
Introduction: Secure Os, Security Goals, Trust Model, Threat Model, Access Control. Fundamentals: Protection system, Lampson's Access Matrix, Mandatory protection system.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

Module-2
Multics: Fundamentals, multics protection system models, multics reference model, multics security, multics vulnerability analysis.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

Module-3
Security in ordinary operating system: UNIX security, windows security Verifiable security goals: Information flow, information flow secrecy, models, information flow integrity model, the challenges of trusted, process, covert channels.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

Module-4
Security Kernels: The Security Kernels, secure communications, processor Scomp, Gemini secure OS, Securing commercial OS, Retrofitting security into a commercial OS, History Retrofitting commercial OS, Commercial era, microkernel era, UNIX era- IX, domain and type enforcement.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

Module-5
Case study: Solaris Extensions Trusted extensions, access control, Solaris compatibility, trusted extensions, mediations process rights management, role based access control, trusted extensions, networking trusted extensions, multilevel services, trusted extensions administration

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Three Unit Tests each of **20 Marks**
2. Two assignments each of **20 Marks** or **one Skill Development Activity of 40 marks**
3. to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:

1. The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
2. The question paper will have ten full questions carrying equal marks.
3. Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
4. Each full question will have a sub-question covering all the topics under a module.
5. The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:

Text Books

1.Operating system security, Trent Jaeger MorganM & Claypool ,Publishers ,2008

 Reference Books

1.Guide to Operating system Security, Michael Palmer Thomson

Web links and Video Lectures (e-Resources):

- https://www.youtube.com/watch?v=ZaGGKFCLNc0

Skill Development Activities Suggested

The students with the help of the course teacher can take up relevant technical –activities which will enhance their skill. The prepared report shall be evaluated for CIE marks.

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Identify and compare different formal security goals and variety of security models proposed for development of secure operating systems.	L2
CO2	Interpret architectures of various secure OS and retrofitting security feature on existing commercial OS's.	L2
CO3	Shows variety of approaches applied to the development & extension services for securing operating systems.	L2

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1			X			X					X	
CO2				X					X			
CO3					X			X			X	

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	PO1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
3	Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.	PO3
4	Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.	PO4
5	Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations	PO5
6	The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering and business practices.	PO6
7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9
10	Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.	PO10
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.	PO11
12	Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.	PO12

@#01112023