CYBER SECURITY AND CYBER LAW			
Course Code	**22SCR13**	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:

- To analyze and evaluate the cyber security needs of an organization.
- To determine and analyze software vulnerabilities and security solutions to reduce the risk of exploitation.
- To design and develop security architecture for an organization.
- To design operational and strategic cyber security strategies and policies.

Module-1

Cyber Security: Introduction in Cyber Security -Hackers - Attackers -Types of Attackers Examples –Data Recovery.

Cyber law: Features of Cyber Law - Significance of Cyber Law - Advantages. Data Security - Meaning - Fundamentals of Data Security - Requirements of Data Security - Precautionary Measures.

Teaching-Learning Process	Chalk and talk/Power point presentation/ Web resources(https://www.coursera.org/learn/cybersecurity-for-everyone)

Module-2

Tools and Methods Used in Cyber crime: Proxy Servers and Anonymizers, Phishing, Password Cracking, Key loggers and Spywares, Virus and Worms, Steganography, DoS DDoS Attacks, SQL Injection, Buffer Over Flow, Attacks on Wireless Networks, Phishing, Identity Theft (ID Theft)Cybercrimes and Cyber security: The Legal Perspectives Why do we need Cyber law: The Indian Context, The Indian IT Act, Digital Signature and the Indian IT Act, Amendments to the Indian IT Act, Cybercrime and Punishment, Cyber law, Technology and Students: Indian Scenario.

Teaching-Learning Process	Chalk and talk/ Power point presentation/ Use SIFT Workstation (open-source network software)/ Assignment

Module-3

Authentication and Firewalls - Authentication & Access Control: Identification - Authentication - Authentication by Passwords - Protecting Passwords - Access Control Structure - Evidences - Law of Evidence on Electronic Records,

Hackers & its Types - Cracking - Pornography - Software privacy - Data Recovery - File Modification & File access, Recover Internet Usage Data, Recover Swap Files/Temporary/Cache Files, and Introduction to Encase Forensic.

Teaching-Learning Process	Chalk and talk/Power point presentation Usage of Firewall Tool/ Web resources.

Module-4	
Cyber security: Organizational Implications Cost of Cybercrimes and IPR Issues: Lesson for Organizations, Web Treats for Organizations: The Evils and Perils, Security and Privacy Implications from Cloud Computing, Social Media Marketing: Security Risk and Perils for Organization, Social Computing and the Associated Challenges for Organizations, Protecting People's Privacy in the Organization, Organizational Guidelines for Internet Usage, Safe Computing Guidelines and Computer Usage Policy, Incident Handling: An Essential Component, Intellectual Property rights in the Cyber security, Importance of Endpoint Security in Organizations.	
Teaching-Learning Process	Chalk and talk/ Power point presentation/ Classroom Interaction/ Assignment
Module-5	
Concept of Cyber law and Cyber Space: Introduction - Meaning and Features of Cyber law - Significance and Advantages of Cyber Law - Meaning of Cyber Space - Inclusive of Cyber Space - Facilitating Functions of Cyber Space - Major Issues in Cyber Space. Need for an Indian Cyber law: Plans of National Information Technology Policy (NITP) - Need for Protection of data - Transactions in Security - Electronic Banking.	
Teaching-Learning Process	Chalk and talk/Power point presentation/Classroom Interaction, Web resources: (https://www.udemy.com/course/cybersecurity-law-policy)

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 Evluation) 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:
TextBooks:

1. Jonathan Rosenoer , Cyber law: The Law of Internet, Springer Verlog, Paperback, 17 September 2011
2. John W Ritting House, William M.Hancock, Cyber Security Operations Handbook, Read Elsevier,2004

Reference Books:

1. Sunit Belapure and Nina Godbole. Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives. Wiley India Pvt Ltd. 2013.
2. Surya PrakashTripathi, Ritendra Goyal, Praveen Kumar Shukla. Introduction to information security and cyber laws. Dreamtech Press. 2015.
3. Cybersecurity Essentials
4. Charles J. Brooks, Christopher Grow, Philip A. Craig Jr., Donald Short, ISBN: 978-1-119-36239-5 October 2018.

Web links and Video Lectures (e-Resources)

- https://www.udemy.com/course/cybersecurity-law-policy
- https://academy.apnic.net/en/course/introduction-to-cybersecurity
- https://www.coursera.org/specializations/intro-cyber-security
- https://www.coursera.org/learn/cybersecurity-for-everyone
- https://www.classcentral.com/tag/cybercrime

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Define and identify the cyber security needs of an organization.	L1
CO2	Predict and analyze the software vulnerabilities and security solutions to reduce the risk of exploitation.	L2
CO3	Identify the cyber crime and modify security architecture for an organization.	L3
CO4	Survey operational and strategic cyber security strategies and policies	L4(Through Assignment)

Mapping of COs and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	X											
CO2				X								
CO3			X									
CO4	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 AND CLOUD SECURITY			
Course Code	**22SCR14**	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 define the Security associated with computer networks.
- To describe various communications networks and their main components.
- To identify the benefits and characteristics of cloud computing.
- To describe the various virtualization techniques and vulnerabilities.

Module-1

Wireless Network security: Wireless security, Wireless network threats, Wireless network measures, mobile device security, security threats, mobile device security strategy, IEEE 802.11 Wireless LAN overview, the Wi-Fi alliance, IEEE 802 protocol architecture. Security, IEEE 802.11i services, IEEE 802.11i phases of operation, discovery phase, Authentication phase, key management phase, and protected data transfer phase, the IEEE 802.11i pseudorandom function. Web Security Considerations: Web Security Threats, Web Traffic Security Approaches. Secure Sockets Layer: SSL Architecture, SSL Record Protocol, Change Cipher Spec Protocol, Alert Protocol, and shake Protocol, Cryptographic Computations. Transport Layer Security: Version Number, Message Authentication Code, Pseudorandom Functions, Alert Codes, Cipher Suites, Client Certificate Types, Certificate Verify and Finished Messages.

Teaching-Learning Process	Chalk and Talk/ Power point presentation/Classroom Interaction/Web resources(https://wiki.apnictraining.net/netsec20220505-online)

Module-2

Electronic Mail Security: Pretty good privacy, notation, operational; description, S/MIME, RFC5322, Multipurpose internet mail extensions, S/MIME functionality, S/MIME messages, S/MIME certificate processing, enhanced security services, Domain keys identified mail, internet mail architecture, E-Mail threats, DKIM strategy, DKIM functional flow. IP Security: IP Security overview, applications of IPsec, benefits of IPsec, Routing applications, IPsec documents, IPsec services, transport and tunnel modes, IP Security policy, Security associations, Security associations database, Security policy database, IP traffic processing, Encapsulating Security payload, ESP format, encryption and authentication algorithms, Padding, Anti replay service, transport and tunnel modes, combining security associations, authentication plus confidentiality, basic combinations of security associations, internet key exchange, key determinations protocol, header and payload formats, cryptographic suits.

Teaching-Learning Process	Chalk and Talk/ Power point presentation/ Assignment

Module-3

	Cloud Computing Architectural Framework: Cloud Benefits, Business scenarios, Cloud Computing Evolution, cloud vocabulary, Essential Characteristics of Cloud Computing, Cloud deployment models, Cloud Service Models, Multi- Tenancy, Approaches to create a barrier between the Tenants, cloud computing vendors, Cloud Computing threats, Cloud Reference Model, The Cloud Cube Model, Security for Cloud Computing, How Security Gets Integrated	
	Teaching-Learning Process	Chalk and Talk/ Power point presentation using Diagrams/web resources (https://www.geeksforgeeks.org/architecture-of-cloud-computing/)
	Module-4	
	Compliance and Audit: Cloud customer responsibilities, Compliance and Audit Security Recommendations. Portability and Interoperability: Changing providers reasons, Changing providers expectations, Recommendations all cloud solutions, IaaS Cloud Solutions, PaaS Cloud Solutions, SaaS Cloud Solutions.	
	Teaching-Learning Process	Chalk and Talk/ Power point presentation/Article (about cloud customer recommendations and responsibilities)
	Module-5	
	Identity and Access Management: Identity and Access Management in the cloud, Identity and Access Management functions, Identity and Access Management (IAM) Model, Identity Federation, Identity Provisioning Recommendations, Authentication for SaaS and Paas customers, Authentication for IaaS customers, Introducing Identity Services, Enterprise Architecture with IDaaS , IDaaS Security Recommendations. Virtualization: Hardware Virtualization, Software Virtualization, Memory Virtualization, Storage Virtualization, Data Virtualization, Network Virtualization, Virtualization Security Recommendations.	
	Teaching-Learning Process	Chalk and Talk/ Power point presentation/ Assignment about Diff virtualization

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 Evluation) 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. William Stallings, Cryptography and Network Security Principles and security, Pearson 7th edition, 2017.
2. Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, Oreilly Media.2009.

Reference Books:

1. J. R. Vic Winkler, Securing the Cloud, Cloud Computer Security Techniques and Tactics, Syngress, 2014

Web links and Video Lectures (e-Resources):

- https://wiki.apnictraining.net/netsec20220505-online
- https://wiki.apnictraining.net/netsec20190923-mo
- https://www.udemy.com/courses/it-and-software/network-and-security
- https://www.netacad.com/courses/cybersecurity/network-security
- https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiOgoXW7p36AhUi2DgGHR3RAoUQwqsBegQIKRAB&url=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3Dyr1Psapupsc&usg=AOvVaw1NnvArKyDjDU_XgkKthSvL
- https://www.coursera.org/courses?query=cloud%20security
- https://www.youtube.com/watch?v=Ijkvx1u0w6o

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 the security issues in the network and resolve it.	L1
CO2	Illustrate the different types of cloud solutions among IaaS, PaaS, SaaS.	L3
CO3	Define the recommendations for using and managing the customer's identity and choose the type of virtualization to be used	L1
CO4	Analyze the vulnerabilities in any computing system and hence be able to choose a security solution.	L4(through Assignment)

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												
CO3				X								
CO4	X											

ETHICAL HACKING			
Course Code	**22SCR15**	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:

- Describe about the foot printing and Enumeration techniques.
- Demonstrate the encrypting file system and folder permission.
- Identify the hacking and different type of hacking.
- Discuss the types of attacks and services.

Module-1

Introduction to ethical hacking: Fundamentals of computer networking. TCP/IP protocol stacks. Casing the Establishment**:** What is foot printing, Internet Foot printing, Scanning, Enumeration, basic banner grabbing, Enumerating Common Network services. Case study: Network Security Monitoring.

Teaching-Learning Process	Chalk and talk/ Power point presentation/ Case study discussion. /Video Demonstration: https://onlinecourses.nptel.ac.in/noc19_cs68/preview

Module-2

Securing permission: Securing file and folder permission, Using the encrypting file system, Securing registry permissions. Securing service: Managing service permission, Default services in windows 2000. Unix: The Quest for Root, Remote Access vs Local access, Remote access, Local access, After hacking root.

Teaching-Learning Process	Chalk and talk/ Power point presentation/Web resources, Give an assignment for write an article about file and folder permission & encryption.

Module-3

VPN hacking, VoIP Spoofing, GPS Spoofing, Brute-Force Scripting, Voice mail hacking, VPN hacking, Network Devices: Discovery Autonomous System Lookup, Social Media, Service Detection, Network Vulnerability, Detecting Layer 2 Media.

Teaching-Learning Process	Chalk and talk/Power point presentation/ Show and demonstrate the types of hacking/ Web resources. (https://www.geeksforgeeks.org/types-of-hacking)

Module-4

Wireless Hacking: Wireless Foot printing, Wireless Scanning and Enumeration, Gaining Access, Tools that exploiting WEP Weakness, Denial of Services Attacks, Firewalls: Firewalls landscape, Firewall Identification Scanning Through firewalls, packet Filtering, Application Proxy Vulnerabilities, Denial of Service Attacks, Motivation of Dos Attackers, Types of DoS attacks, Generic Dos Attacks, UNIX and Windows DoS, DDoS.

	Teaching-Learning Process	Chalk and talk/Power point presentation/ Show the Tool usage for foot printing/ Assignment: write an article about Firewall
	Module-5	
	Remote Control Insecurities: Discovering Remote Control Software, Connection, Weakness.VNC, Microsoft Terminal Server and Citrix ICA, Advanced Techniques Session Hijacking, Back Doors, Trojans, Cryptography, Subverting the systems Environment, Social Engineering, Web Hacking, Web server hacking web application hacking, Hacking the internet Use, Malicious Mobile code, SSL fraud, E-mail Hacking, IRC hacking, Global countermeasures to Internet User Hacking. APT case study	
	Teaching-Learning Process	Chalk and talk/ Power point presentation Classroom Interaction/ Web resources.

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. Stuart McClure, Joel Scambray and Goerge Kurtz , Hacking Exposed 7: Network Security Secrets & Solutions,Tata McGraw Hill Publishers, 2012
2. Kit Bensmith, and Brian Komer ,Microsoft Windows Security Resource Prentice Hall of India

Reference Books

1. Gray Hat Hacking The Ethical Hackers Handbook Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle McGraw-Hill Osborne Media paperback 3rd Edition.2011

Web links and Video Lectures (e-Resources):

- https://www.simplilearn.com/cyber-security/ceh-certification?utm_source=google&utm_medium=cpc&utm_term=&utm_content=1632205197-79872225071-377654317159&utm_device=c&utm_campaign=Search-TechCluster-Cyber-OthersNew-IN-Main-AllDevice-adgroup-DSA-Category-Page&gclid=CjwKCAjwg5uZBhATEiwAhhRLHpJKcI-8Jzytg1p9ByQBrSs1Pc5R0GcklMm-sGq3foLJah3xJ0z3lhoCSPMQAvD_BwE.
- https://hackr.io/blog/best-ethical-hacking-courses
- https://www.udemy.com/topic/ethical-hacking
- https://onlinecourses.nptel.ac.in/noc19_cs68/preview

Skill Development Activities:
Practically learn the usage of Burp Suite and Netsparker tool.

- https://www.hackerone.com/ethical-hacker/100-hacking-tools-and-resources
- (https://www.mygreatlearning.com/blog/ethical-hacking-tools)
- (https://www.softwaretestinghelp.com/ethical-hacking-tools)

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Explain aspects of security, importance of data gathering, foot printing and system hacking.	L2
CO2	Recall and list the Default services in windows 2000 .	L1
CO3	Use the encrypting file system, Securing file and folder permission.	L3
CO4	Apply hacking technique and detect the different types of attacks.	L3

Mapping of COs and Pos

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

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**oneSkill 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. *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

ETHICAL HACKING LABORATORY			
Course Code	**22SCRL17**	CIE Marks	50
Teaching Hours/Week (L:T:P: S)	1:2:0	SEE Marks	50
Credits	02	Exam Hours	03

Course objectives:

- To practice and Evaluate modern tools.
- To analyze packet capturing in network.
- To define forensic analysis.
- To identify and provide the Security in various web applications.

Sl. NO	Experiments
1	Wireshark: Experiment to monitor live network capturing packets and analyzing over the live network.
2	LOIC: DoS attack using LOIC
3	FTK: Bit level forensic analysis of evidential image and reporting the same
4	Darkcomet : Develop a malware using Remote Access Tool Darkcomet to take a remote access over network.
5	HTTrack: Website mirroring using Httrack and hosting on a local network
6	XSS: Inject a client side script to a web application.
7	Email tracker pro: Email analysis involving header check, tracing the route. Also perform a check on a spam mail and non-spam mail.
	Demonstration Experiments (For CIE) if any
9	Detect ARP spoofing using open source tool ARPWATCH.
10	Use the Nessus tool to scan the network for vulnerabilities.
11	Implement a code to simulate buffer overflow attack

Course outcomes (Course Skill Set):

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

- Select modern tools for identify the hacking.
- Analyze packet capturing in network
- Identify forensic, hacking and security crime.
- Provide Security in various web applications

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 8^{th} week of the semester and the second test shall be conducted after the 14^{th} 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

Suggested Learning Resources:

- https://www.udemy.com/topic/ethical-hacking/
- https://hackr.io/blog/best-ethical-hacking-courses
- https://youtu.be/dz7Ntp7KQGA
- https://youtu.be/6wKONaS1t2Q
- https://youtu.be/CSqa9__JrzU

	Web Application and Database Security			
	Course Code	**22SCR21**	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 identify and aid in fixing any security vulnerabilities during the web development process.
- To provide the security principles in developing a reliable web application.
- To emphasize the underlying principles of Relational Database Management System.
- To model and design advanced data models to handle threat issues, security and counter measures for web application.

Module-1

Overview of Web Applications: Introduction history of web applications interfaces ad structure benefits and drawbacks of web applications Web application Vs Cloud application**.**

Web Application Security Fundamentals: Security Fundamentals: Input Validation - Attack Surface Reduction Rules of Thumb- Classifying and Prioritizing Threads.

Cutting Edge Web Application Security: DNS rebinding - Flash security - Java applet security - Single-sign-on solution and security - IPv6 impact on web security.

Teaching-Learning Process	Demo: Use industry standard tools for web application security. Case study of zero click attack https://www.youtube.com/watch?v=j5PuYFCS0Iw

Module-2

Browser Security Principles: Origin Policy - Exceptions to the Same-Origin Policy - Cross-Site Scripting and Cross-Site Request Forgery - Reflected XSS - HTML Injection.

Web Application Vulnerabilities: Understanding vulnerabilities in traditional client server application and web applications, client state manipulation, cookie based attacks, SQL injection, cross domain attack (XSS/XSRF/XSSI) http header injection. SSL vulnerabilities and testing - Proper encryption use in web application - Session vulnerabilities and testing - Cross-site request forgery.

Teaching-Learning Process	https://www.youtube.com/watch?v=cH6TbFOikFU https://www.youtube.com/watch?v=loyVGklGpjU

Module-3

Web Application Mitigations: Http request , http response, rendering and events , html image tags, image tag security, issue, java script on error , Javascript timing , port scanning , remote scripting , running remotecode, frame and iframe , browser sandbox, policy goals, same origin policy, library import, domain relaxation.

Secure Website Design: Architecture and Design Issues for Web Applications, Deployment Considerations Input Validation, Authentication, Authorization, Configuration Management ,Sensitive Data, Session Management, Cryptography, Parameter Manipulation, Exception Management, Auditing 5 hours and Logging, Design Guidelines, Forms and validity, Technical implementation.

Teaching-Learning Process	https://www.youtube.com/watch?v=CQZxeoQeo5c Through Website Design.

Module-4

	Database security-Introduction includes threats, vulnerabilities and breaches, Basics of database design, DB security, concepts, approaches and challenges, types of access controls, Oracle VPD. **Discretionary and Mandatory access control**-Principles, applications and poly instantiation, Database inference problem, types of inference attacks, distributed database, security levels, SQL-injection: types and advanced concepts.	
	Teaching-Learning Process	PPT/Article: give an assignment for write article about importance about Database and web application security.
	Module-5	
	Security in Relational Data Model-Security in relational data model, concurrency controls and locking, SQL extensions to security (oracle as an example), System R concepts, Context and control based access control, Hippocratic databases, Database watermarking, Database intrusion, secure data outsourcing.	
	Teaching-Learning Process	Chalk and Talk/ PPT/Web resources: https://www.youtube.com/watch?v=B7Y9c7bpHds

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:

TextBooks:

1. Sullivan, Bryan, and Vincent Liu. Web Application Security, A Beginner's Guide. McGraw Hill Profe ssional, 2011.
2. Alfred Basta, Melissa Zgola, "Database Security", Course Technology, 2012

Reference Books:

1. Bhavani Thuraisingham, "Database and Applications Security", Integrating Information Security and Data Management, Auerbach Publications, 2005.
2. Stuttard, Dafydd, and Marcus Pinto. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. John Wiley Sons, 2011.
3. Michael Gertz and Sushil Jajodia, "Handbook of Database Security— Applications and Trends", Springer, 2008.

Web links and Video Lectures (e-Resources):

- https://www.youtube.com/watch?v=qjrkV4RjgIU
- https://www.youtube.com/watch?v=B-ytMSuwbf8
- https://www.youtube.com/watch?v=nPZp-YNPyC8
- https://www.youtube.com/watch?v=j5PuYFCS0Iw
- https://www.youtube.com/watch?v=HMbEk3_fNH0
- https://heimdalsecurity.com/blog/web-application-security
- https://www.udemy.com/course/web-application-security

Skill Development Activities Suggested

- Create your own web application and database security.

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Identify the various types of threats and vulnerabilities in the web applications	L1
CO2	Select the security principles in developing a reliable web application	L1
CO3	Discuss the importance of web application and database security	L2
CO4	Modify or update the security of own organizations database or company database.	L3

Mapping of COS and POs

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

Semester - II

Defensive Security			
Course Code	**22SCR22**	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	03

Course objectives:

- To develop a foundational set of guidelines, standards, and practises
- To explore automated process and tools for vulnerability management
- To securely develop code to reduce exploitable errors

MODULE-1	
Defense Logistics: The Military Contract Service Model, Critical Review and Intervention Measures, Contract service model, Incentive scheme, Recruitment Retention, Reintegration. A Maritime Vision for Geopolitics: Geopolitics, Maritime interests. Maritime Security and Safety: Comprehensive Security in Artisanal Fisheries, Comprehensive security, Artisan fishing, State, Society, Artisanal fishermen. Offshore Wind Farms – Support or Threat to the Defence of Polish Sea Areas: Offshore planning, Offshore wind farms, Opto-electronic head, Surveillance radar, Acoustic barrier.	
Teaching-Learning Process	Chalk and Talk/ PPT

MODULE-2	
Naval and Military Engineering: Horseshoe Vortex Suppression- Strake, Horseshoe vortex, Junction vortex. Hybrid Joint Between Steel Deck and Fiberglass Superstructure- Hybrid joint, Composite panel, Composite superstructure.	
Teaching-Learning Process	Chalk and Talk/ PPT/Assignment

MODULE-3	
Security in the Storage of Ammunitions and Explosives in Ecuador: Storage of ammunitions, Explosives, Physical security. Engineering Analysis and Signal Processing: Interference of Biological Noise in Sonar Detection- Sonar, Noise, Noise mapping, Information system, Data Mining.	
Teaching-Learning Process	Chalk and Talk/ PPT

MODULE-4	
Creating a Security Program and Asset Management and Documentation: Assess Threats and Risks , Information Classification Asset Management Implementation Steps, Standards and Procedures. Incident Response, Processes, Tools and Technology. Disaster Recovery: Recovery Strategies.	
Teaching-Learning Process	Chalk and Talk/ PPT/Assignment

MODULE 5

Physical Security: Physical, Operational. Password Management and Multifactor Authentication: Password Management Software, Password Resets, Password Breaches, Encryption, Hashing, and Salting. Password Storage Locations and Methods, Password Security Objects: Setting a Fine-Grained Password Policy.	
Teaching-Learning Process	Chalk and Talk/ PPT/Seminar

PRACTICAL COMPONENT OF IPCC

Sl.NO	Experiments
1	Defense against Query-based Hard-label Attack: Propose a practical and generalizable defensive framework against black-box query-based hard-label at-tacks via invalidating the essential gradient estimation step. PredCoinis a certifiable defense, fundamentally supported by analytical reasoning on this invalidation process.
2	To the above query do perform extensive experiments under various tasks and settings to evaluate PredCoin against four state-of-the-art QBHL attacks. Results show PredCoin significantly improves the robustness of the model against QBHL attacks in both`2and`∞settings, even assuming an excessive query budget (50K queries).

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. The15 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 experimentsshall 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:

Books

1. "Developments and Advances in Defense and Security", Alvaro Rocha, Teresa Guarda, Springer 1st edition, 2018.
2. "Defensive Security Handbook", Lee Brotherston, Amanda Berlin, O'Reilly Media, 2017

Web links and Video Lectures (e-Resources):

1. https://www.youtube.com/watch?v=ZHz-Lj7m-8s
2. https://www.youtube.com/watch?v=25GL3T-pLxs

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning

1. https://www.digitaldefense.com/solution-overview/educate/

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Create a base set of policies, standards, and procedures	L2
CO2	Investigate automated techniques and tools for managing vulnerabilities	L4
CO3	Write code to minimise exploitable flaws.	L4,L5

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								

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

SECURITY ARCHITECTURE DESIGN			
Course Code	**22SCR231**	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 Identify the components targeted for each zone
- To Summarize the Map site zones with level of security
- To Analyze the secured sites based on tools & techniques

Module-1

Architecture and Security: Architecture Reviews, Software Process, Reviews and the Software Development Cycle, Software Process and Architecture Models, Software Process and Security, Architecture Review of System, Security Assessments, Security Architecture Basics, Architecture Patterns in Security

Teaching-Learning Process	Chalk and Talk/PPT /web resource: https://www.youtube.com/watch?v=LREcVbHiqTo

Module-2

Low-Level Architecture: Code Review, importance of code review, Buffer Overflow Exploits, Countermeasures Against Buffer Overflow Attacks, patterns applicable, Security and Perl, Bytecode Verification in Java-Good Coding Practices Lead to Secure Code, Cryptography, Trusted Code, Secure Communications.

Teaching-Learning Process	Chalk and Talk/PPT/Assignment

Module-3

Mid-Level Architecture: Middleware Security, Middleware and Security, The Assumption of Infallibility, The Common Object Request Broker Architecture, The OMG CORBA Security Standard, Vendor Implementations of CORBA Security, CORBA Security Levels, Secure Interoperability, Application, Unaware Security, Application, Aware Security, Application Implications, Web Security, Application and OS Security, Database Security.

Teaching-Learning Process	Chalk and Talk/PPT/Assignment

Module-4

High-Level Architecture: Security Components, Secure Single Sign-On- Public-Key Infrastructures, Firewalls, Intrusion Detection Systems, LDAP and X.500 Directories, Kerberos, Distributed Computing Environment,The Secure Shell, or SSH, The Distributed Sandbox, Security and Other Architectural Goals, Metrics for Non-Functional Goals, Force Diagrams around Security, High Availability, Robustness, Reconstruction of Events, Ease of Use, Maintainability, Adaptability, and Evolution, Scalability, Interoperability, Performance, Portability.

	Teaching-Learning Process	Chalk and Talk/PPT/Assignment/Seminar

	Module-5
	Enterprise Security Architecture: Security as a Process, Security Data, Enterprise Security as a Data Management Problem, Tools for Data Management, David Isenberg and the "Stupid Network", Extensible Markup Language,The XML Security Services Signaling Layer, XML and Security Standards, The Security Pattern Catalog Revisited, XML-Enabled Security Data-HGP: A Case Study in Data Management, Business Cases and Security, Building Business Cases for Security Case study: Building secure OS for Linux: Linux security modules, security enhanced Linux

	Teaching-Learning Process	Chalk and Talk/PPT/Assignment/Seminor

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 Book:

1. Jay Ramachandran, Designing Security Architecture Solutions Wiley Computer Publishing 2010.

Reference Book:

1. Markus Schumacher, Security Patterns: Integrating Security and Systems Engineering Wiley Software Pattern Series 2010.

Web links and Video Lectures (e-Resources):

- https://www.youtube.com/watch?v=LREcVbHiqTo
- https://www.youtube.com/watch?v=4qN3JBGd1g8
- https://www.youtube.com/watch?v=LDQxzz42Bs0

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 the components targeted for each zone	L1
CO2	Summarize the Map site zones with level of security	L2
CO3	Analyze the secured sites based on tools & techniques	L4

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

SECURITY ASSESSMENT AND AUDIT			
Course Code	**22SCR232**	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 illustrate the roles information security and its management.
- To select appropriate techniques to tackle and solve problems in the discipline of information security assessment.
- To design an information security and validation system.

Module-1

Evolution of information security: information assets, security standards, organizational impacts, security certifications, elements of information security program, need for security assessment, security assessment process.

Teaching-Learning Process	Chalk and Talk/ PPT/ Web Resources: https://www.youtube.com/watch?v=_s6qDjgCbCE

Module-2

Security assessment planning: Business drivers, scope definition, consultant's perspective, Client's perspective, Development of project plan. Initial information gathering, Initial preparation, analysis of gathered information.

Teaching-Learning Process	Chalk and Talk/ PPT/Article

Module-3

Business process evaluation, Technology evaluation, Risk analysis, Risk mitigation.

Teaching-Learning Process	Chalk and Talk/ PPT/Seminar

Module-4

Security Risk assessment project management, Security risk assessment approaches and methods.

Teaching-Learning Process	Chalk and Talk/ PPT/ Assignment

Module-5

Information security standards, Information security Legislation, Formal security verification, Security verification with SSL.

Teaching-Learning Process	Chalk and Talk/ PPT/ Web Resources: https://www.youtube.com/watch?v=I8KqFI8CuNk

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. A practical guide to security assessments Sudhanshu Kairab CRC press 2005
2. A Security risk assessment Handbook Douglas J. Landoll Auerbach publications 2006

Reference Books:

1. Principles of Information Security Michael E. Whitman, Herbert J. Mattord Cengage Learning 2nd Edition

Web links and Video Lectures (e-Resources):

- https://www.youtube.com/watch?v=_s6qDjgCbCE
- https://www.youtube.com/watch?v=I8KqFI8CuNk
- https://www.youtube.com/watch?v=ZsUs8pMyTOs
- https://www.youtube.com/watch?v=W2jo68AbUH0

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	Select appropriate techniques to tackle and solve problems in the discipline of information security assessment	L1
CO2	Illustrate the roles information security and its management	L3
CO3	Design an information security and validation system	L6

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

Blockchain Technology			
Course Code	**22SCR233**	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 crypto currency, Along with the Decentralization.
- To recognise the bitcoin alternatives and Smart Contracts and Ethereum.

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**oneSkill 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.

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

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			x					
CO2	x			x								
CO3		x								x		

Information Security Policies in Industry			
Course Code	**22SCR234**	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 explain the content, need, and responsibilities of information security policies.
- To explain the standards, guidelines, Procedures, and key roles of the organization.
- To write policy document for securing network connection and interfaces.
- To explain the threats to the stored data or data in transit and able to write 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

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/Assignment

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/Seminar

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/Assignment

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-Learning Process	Chalk and talk, PPT/ Seminar

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.

Suggested Learning Resources:

TextBooks

1. Scott Barman. Writing Information Security Policies. Sams Publishing. 2002.
2. Thomas.R.Peltier. Information Policies Procedures and Standards. Thomas.R.Peltier. CRC Press. 2004.

Reference Books:

1. Thomas R Peltier, Justin Peltier, John Backley. Information Security Fundamentals. CRC Press,2005.
2. Harold F. Tipton and Micki Krause. Information Security Management Handbook. Auerbach publications. 5th Edition, 2005.

Web links and Video Lectures (e-Resources):

- https://www.udemy.com/topic/information-security/

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 content, need, and responsibilities of information security policies.	L2
CO2	Identify the threats to the stored data or data in transit and able to write policy document	L1
CO3	Describe the standards, guidelines, Procedures, and key roles of the organization.	L2
CO4	Summarize policy document for securing network connection and interfaces.	L2

Mapping of COS and Pos

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

CYBER THREAT SIMULATION MANAGEMENT			
Course Code	**22SCR235**	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 identify different types of threats for management.
- To recognize the vulnerability in the digital society.
- To use trends and identifying the risk councils and worst occurs.

Module-1

The Cyber Threat to the Corporate Brand: The Rise of Cyber Organized Crime and Its Global Impact, Is Nothing Sacred? The Liberty Reserve Case: Money Laundering in the Digital Age, The Corruption Factor, Information Threat, Physical Threat, The Emergence of the Cyber Nation-State and Technology Espionage, A Case of Cyber Espionage Conspiracy? According to the Select Committee…

Teaching-Learning Process	Chalk and Talk/ PPT/ Web Resources https://www.youtube.com/watch?v=WRIakA5CP3I

Module-2

Corporate Vulnerabilities in the Digital Society: What Is the True Cost of a Cyber Attack? Cyber Attack Detection Sometimes Takes Years, One of the First Questions: "How Much Will This Cost?"A Few Common Cost Factors, What About Unreported Breaches? Cyber Attacks Result in a Wider Impact: The Community, U.S. Cyber Public Policy, No Guarantees with this Executive Order, Government-Industry Cooperation: No Silver Bullet, The Challenge of Defining Cyber Public Policy, Cold War II: The Cyber Chapter, Is There a Silver Lining in an Attack?

Teaching-Learning Process	Chalk and Talk/ PPT/ Assignment

Module-3

Four Trends Driving Cyber Breaches and Increasing Corporate Risk:
Technology Trend, Loss of Situational Awareness: Distraction, Culture, Technology is a Double-Edged Sword, Social Media and Digital Protest, Social Media: A Tool for Disruption, a Model for Change, The Hacker Group Anonymous, Anarchaos: In the Image of Anonymous.

Teaching-Learning Process	Chalk and Talk/ PPT/Seminar

Module-4

Managing the Brand When the Worst Occurs: Be Prepared, Managing the Big Risk, Background Investigation Suggestions to Improve Process, Risk-Reinforced Service Level Agreements, Clouds Fill the Horizon.

Teaching-Learning Process	Chalk and Talk/ PPT/Article

Module-5

	Creating Executive Cyber Risk Councils: The Goal of the Executive Cyber Risk Council, Who Should be Included in the Executive Risk Council? Early Warnings, Technical Signals Are There—But You've Got to Look, Know Who's Inside the Enterprise, What a Web we Weave… When Surfing.	
	Teaching-Learning Process	Chalk and Talk/ PPT/Seminar

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:

TextBook:

1. Cyber Threat!: How to Manage the Growing Risk of Cyber Attacks by MacDonnell Ulsch,Wiley, 2014

Reference Book:

1. Jerry M. Couretas , An Introduction to Cyber Modeling and Simulation,Wiley, 2018

Web links and Video Lectures (e-Resources):

- https://www.tonex.com/training-courses/cyber-threat-simulation-training/
- https://www.youtube.com/watch?v=7Y6o8-0U7Mk
- https://www.youtube.com/watch?v=YoXgTC_yMH4

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	Describe the different types of threats for management.	L2
CO2	Recognize the vulnerability in the digital society.	L1
CO3	Use trends and identifying the risk councils and worst occurs	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

DEEP LEARNING			
Course Code	**22SCR241**	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 objectives:

- To identify the context of neural networks and deep learning.
- To recognise how to use a neural network.
- To summarize the data needs of deep learning.
- To explore the working knowledge and the parameters of neural networks and deep learning.

MODULE-1

Machine Learning Basics: Learning Algorithms, Capacity, Over fitting and Under fitting, Hyper parameters and Validation Sets, Estimator, Bias and Variance, Maximum Likelihood Estimation, Bayesian Statistics, Supervised Learning Algorithms, Unsupervised Learning Algorithms, Stochastic Gradient Descent, building a Machine Learning Algorithm, Challenges Motivating Deep Learning.

Teaching-Learning Process	Chalk and board and PPT/web resources: https://www.youtube.com/watch?v=NOJOYcmyDhM

MODULE-2

Deep Feed forward Networks: Gradient-Based Learning, Hidden Units, Architecture Design, Back Propagation. Regularization: Parameter Norm Penalties, Norm Penalties as Constrained Optimization, Regularization and Under-Constrained Problems, Dataset Augmentation, Noise Robustness, Semi Supervised Learning, Multi-Task Learning, Early Stopping, Parameter Tying and Parameter Sharing, Sparse Representations, Bagging, Dropout.

Teaching-Learning Process	Chalk and board and PPT/Assignment

MODULE-3

Optimization for Training Deep Models: How Learning Differs from Pure Optimization, Challenges in Neural Network Optimization, Basic Algorithms. Parameter Initialization Strategies, Algorithms with Adaptive Learning Rates. **Convolutional Networks:** The Convolution Operation, Motivation, Pooling, Convolution and Pooling as an Infinitely Strong Prior, Variants of the Basic Convolution Function, Structured Outputs, Data Types, Efficient Convolution Algorithms, Random or Unsupervised Features.

Teaching-Learning Process	Chalk and board and PPT/ web resources: https://www.youtube.com/watch?v=zfiSAzpy9NM

MODULE-4

Sequence Modelling: Recurrent and Recursive Nets: Unfolding Computational Graphs, Recurrent Neural Networks, Bidirectional RNNs, Encoder-Decoder Sequence-to-Sequence Architectures, Deep Recurrent Networks, Recursive Neural Networks. Long short-term memory

Teaching-Learning Process	Chalk and board and PPT/Seminar

MODULE 5

Practical Methodology: Performance Metrics, Default Baseline Models, Determining Whether to Gather More Data, Selecting Hyperparameters, Debugging Strategies, Example: Multi-Digit Number Recognition. Applications: Vision, NLP, Speech.

Teaching-Learning Process	Chalk and board and PPT/Article/Assignment

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:

TextBooks:

1. Deep Learning Lan Good fellow and YoshuaBengio and Aaron Courville MIT Press, 2016.

Reference books:

1. Neural Networks:Asystematic Introduction Raúl Rojas 1996.
2. Pattern Recognition and machine Learning Chirstopher Bishop 2007.

Web links and Video Lectures (e-Resources):

- https://www.d eeplearningboo k.org/
- https://www.youtube.com/watch?v=VyWAvY2CF9c
- https://www.youtube.com/watch?v=njKP3FqW3Sk
- https://www.youtube.com/watch?v=zfiSAzpy9NM

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 the deep learning algorithms which are more appropriate for various types of learning tasks in various domains.	L1
CO2	Implement deep learning algorithms and solve real-world problems.	L4
CO3	Execute performance metrics of Deep Learning Techniques.	L4

COs and POs Mapping:

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

NATURAL LANGUAGE PROCESSING			
Course Code	**22SCR242**	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 recognise the fundamental concepts and techniques of NLP.
- To Summarize the computational properties of natural languages
- To Design commonly used algorithms for processing linguistic information.

Module-1	
OVERVIEW AND LANGUAGE MODELING: Overview: Origins and challenges of NLP-Language and Grammar-Processing Indian Languages- NLP Applications-Information Retrieval. Language Modeling: Various grammar- based Language Models-Statistical Language Model.	
Teaching-Learning Process	Chalk and Talk Power point presentation

Module-2	
WORD LEVEL AND SYNTACTIC ANALYSIS: Word Level Analysis: Regular Expressions-FiniteState Automata-Morphological Parsing-Spelling Error Detection and correction-Words and Word classesPart-of Speech Tagging. Syntactic Analysis: Context-free Grammar-Constituency-Parsing-Probabilistic Parsing.	
Teaching-Learning Process	Chalk and Talk Power point presentation Assignment

Module-3	
Extracting Relations from Text: From Word Sequences to Dependency Paths: Introduction, Subsequence Kernels for Relation Extraction, A Dependency-Path Kernel for Relation Extraction and Experimental Evaluation. Mining Diagnostic Text Reports by Learning to Annotate Knowledge Roles: Introduction, Domain Knowledge and Knowledge Roles, Frame Semantics and Semantic Role Labelling, Learning to Annotate Cases with Knowledge Roles and Evaluations. A Case Study in Natural Language Based Web Search: InFact System Overview, The GlobalSecurity.org Experience.	
Teaching-Learning Process	Chalk and Talk Power point presentation Assignment

Module-4

	Evaluating Self-Explanations in iSTART: Word Matching, Latent Semantic Analysis, and Topic Models: Introduction, iSTART: Feedback Systems, iSTART: Evaluation of Feedback Systems, Textual Signatures: Identifying Text-Types Using Latent Semantic Analysis to Measure the Cohesion of Text Structures: Introduction, Cohesion, Coh-Metrix, Approaches to Analysing Texts, Latent Semantic Analysis, Predictions, Results of Experiments. Automatic Document Separation: A Combination of Probabilistic Classification and Finite-State Sequence Modelling: Introduction, Related Work, Data Preparation, Document Separation as a Sequence Mapping Problem, Results. Evolving Explanatory Novel Patterns for Semantically based Text Mining: Related Work, A Semantically Guided Model for Effective Text mining.	
	Teaching-Learning Process	Chalk and Talk Power point presentation/Seminar
	Module-5	
	INFORMATION RETRIEVAL AND LEXICAL RESOURCES: Information Retrieval: Design features of Information Retrieval Systems-Classical, Non classical, Alternative Models of Information Retrieval – valuation Lexical Resources: World Net-Frame Net- Stemmers-POS Tagger-Research Corpora.	
	Teaching-Learning Process	Chalk and Talk Power point presentation/Seminar

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 Natural Language Processing and Information Retrieval TanveerSiddiqui, U.S. Tiwary Oxford University Press 2008.

2 Anne Kao and Stephen R. Potee Natural LanguageProcessing andText Mining Springer-Verlag London Limited 2007

3 Speech and Language Processing: Anintroduction to Natural Language Processing, Computational Linguistics and SpeechRecognition Daniel Jurafsky and James H Martin Prentice Hall 2008 2nd Edition

4 Natural Language Understanding James Allen Benjamin/Cummingsp ublishing company 2nd edition, 1995

5 Information Storage and Retrieval systems Gerald J. Kowalski and Mark.T. Maybury Kluwer academic Publishers 2000.

6 Natural Language Processing with Python Steven Bird, Ewan Klein, Edward Loper O'Reilly Media 2009

Web links and Video Lectures (e-Resources):

- https://www.tutorialspoint.com/natural_language_processing/index.htm
- https://www.javatpoint.com/nlp
- https://nptel.ac.in/courses/106105158

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Analyse the natural language text.	L2
CO2	Generate the natural language	L2
CO3	Demonstrate Text mining.	L3
CO4	Apply information retrieval techniques	L3

Mapping of COS and POs

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

MANAGING BIG DATA			
Course Code	**22SCR243**	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 objectives:

- To Describe managing big data using Hadoop and SPARK technologies
- To Explain HDFS and MapReduce concepts
- To Identify the tools and Install, configure, then run Hadoop and HDFS

MODULE-1

Hadoop: Data!, Data Storage and Analysis, Querying All Your Data, Beyond Batch, Comparison with Other Systems: Relational Database Management Systems, Grid Computing, Volunteer Computing Hadoop Fundamentals MapReduce A Weather Dataset: Data Format, Analyzing the Data with Unix Tools, Analyzing the Data with Hadoop: Map and Reduce, Java MapReduce, Scaling Out: Data Flow, Combiner Functions, Running a Distributed MapReduce Job, Hadoop Streaming The Hadoop Distributed Filesystem The Design of HDFS, HDFS Concepts: Blocks, Namenodes and Datanodes, HDFS Federation, HDFS High-Availability, The Command-Line Interface, Basic Filesystem Operations, HadoopFilesystems Interfaces.

Teaching-Learning Process	Chalk and Talk/ PPT/ Web Resources: https://youtu.be/5zJt9qAe01w

MODULE-2

YARN: Anatomy of a YARN Application Run: Resource Requests, Application Lifespan, Building YARN Applications, YARN Compared to MapReduce, Scheduling in YARN: The FIFO Scheduler, The Capacity Scheduler, The Fair Scheduler, Delay Scheduling, Dominant Resource Fairness Hadoop I/O Data Integrity, Data Integrity in HDFS, LocalFileSystem, ChecksumFileSystem, Compression, Codecs, Compression and Input Splits, Using Compression in MapReduce, Serialization, The Writable Interface, Writable Classes.

Teaching-Learning Process	Chalk and Talk/ PPT/Article /https://youtu.be/KqaPMCMHH4g

MODULE-3

MapReduce: Developing a MapReduce Application The Configuration API, Combining Resources, Variable Expansion, Setting Up the Development Environment, Managing Configuration, GenericOptionsParser, Tool, and ToolRunner, Writing a Unit Test with MRUnit: Mapper, Reducer, Running Locally on Test Data, Running a Job in a Local Job Runner, Testing the Driver, Running on a Cluster, Packaging a Job, Launching a Job, The MapReduce Web UI, Retrieving the Results, Debugging a Job, Hadoop Logs, Tuning a Job, Profiling Tasks, MapReduce Workflows: Decomposing a Problem into MapReduce Jobs, JobControl, Apache Oozie How MapReduce Works Anatomy of a MapReduce Job Run, Job Submission, Job Initialization, Task Assignment, Task Execution, Progress and Status Updates, Job Completion,

Teaching-Learning Process	Chalk and Talk/ PPT/ Assignment

MODULE-4

MapReduce Types and Formats: MapReduce Types, Input Formats: Input Splits and Record,s Text Input, Binary Input, Multiple Inputs, Database Input (and Output) Output Formats: Text Output, Binary Output, Multiple Outputs, Lazy Output, Database Output, Flume Installing Flume, An Example, Transactions and Reliability, Batching, The HDFS Sink, Partitioning and Interceptors, File Formats, Fan Out, Delivery Guarantees.	
Teaching-Learning Process	Chalk and Talk/ PPT/ Web Resources: https://youtu.be/akvtHY9fJcU
MODULE 5	
Pig Installing and Running Pig, Execution Types, Running Pig Programs, Grunt, Pig Latin Editors, An Example: Generating Examples, Comparison with Databases, Pig Latin: Structure, Statements, Expressions, Types, Schemas, Functions, Data Processing Operators: Loading and Storing Data, Filtering Data, Grouping and Joining Data, Sorting Data, Combining and Splitting Data. Spark An Example: Spark Applications, Jobs, Stages and Tasks, A Java Example.	
Teaching-Learning Process	Chalk and Talk/ PPT/ Web Resources:https://youtu.be/Ihl7DPBAZ1g

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. Hadoop: The Definitive Guide Tom White O'Reilley Third Edition, 2012
2. SPARK: The Definitive Guide MateiZaharia and Bill Chambers Oreilly 2018

Reference Books:

1. Apache Flume: Distributed Log Collection for Hadoop . D'Souza and Steve Hoffman Oreilly 2014.

Web links and Video Lectures (e-Resources):

- https://www.bing.com/search?q=managing+big+data+videos&qs=n&form=QBRE&sp=-1&pq=managing+big+data+videos&sc=9-24&sk=&cvid=CB9847D2F31F4FA691FE82C34FDAD940&ghsh=0&ghacc=0&ghpl=
- https://youtu.be/KcecJfxbd-4
- https://youtu.be/5zJt9qAe01w
- https://youtu.be/S2MUhGA3lEw
- https://youtu.be/akvtHY9fJcU

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	Describe managing big data using Hadoop and SPARK technologies	L2
CO2	Explain HDFS and MapReduce concepts	L2
CO3	Identify the tools and Install, configure, then run Hadoop and HDFS	L1

Mapping of COS and POs

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

MALWARE ANALYSIS AND REVERSE ENGINEERING			
Course Code	**22SCR244**	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 recognize commonly used file formats.
- To identify conditional execution constructs in disassembled files.
- To Use a debugger to monitor program execution.
- To analyze malware samples packed using common packing techniques in GHIDRA/IDA.

Module-1	
BASIC ANALYSIS: Basic Static Techniques, Malware Analysis in Virtual Machines, Basic Dynamic Analysis	
Teaching-Learning Process	Chalk and Talk/ PPT/ Web Resources: https://www.youtube.com/watch?v=f-fMdnUW4X4

Module-2	
ADVANCED STATIC ANALYSIS: : A Crash Course in x86 Disassembly, IDA Pro, Recognizing C Code Constructs in Assembly	
Teaching-Learning Process	Chalk and Talk/ PPT/ Assignment

Module-3	
ADVANCED DYNAMIC ANALYSIS: Analyzing Malicious Windows Programs, Debugging, OllyDbg.	
Teaching-Learning Process	Chalk and Talk/ PPT/Article

Module-4	
MALWARE FUNCTIONALITY: Malware Behavior, Covert Malware Launching, Data Encoding	
Teaching-Learning Process	Chalk and Talk/ PPT/ Assignment

Module-5	
ANTI-REVERSE-ENGINEERING: Anti-Disassembly, Anti-Debugging, Anti-Virtual Machine Techniques	
Teaching-Learning Process	Chalk and Talk/ PPT/Seminar

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 Book:

1. Practical Malware Analysis: The Hands-on Guide to Dissecting Malicious Software" by Michael Sikorski and Andrew Honig (published by No Starch Press, 2012)

Reference Book:

1. The IDA PRO Book: The Unofficial Guide to the World's Most Popular Disassembler, 2nd Edition" by Chris Eagle (published by No Starch Press, 2011.

Web links and Video Lectures (e-Resources):

- https://www.udemy.com/course/malware-analysis-and-reverse-engineering/
- https://ringzer0.training/advanced-malware-analysis.html
- https://www.youtube.com/watch?v=f-fMdnUW4X4
- extension://elhekieabhbkpmcefcoobjddigjcaadp/https://doc.lagout.org/security/Malware%20%26%20Forensics/Practical%20Malware%20Analysis.pdf (Textbook)

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	Recognize commonly used file formats.	L1
CO2	Identify conditional execution constructs in disassembled files.	L1
CO3	Use a debugger to monitor program execution.	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

SECURE PROGRAMMING			
Course Code	**22SCR245**	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 Process	**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	Explain how to respond the security alerts which identifies software issues	L1
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							
CO3				X								
CO4			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 DATABASE SECURITY			
Course Code	**22SCRL26**	CIE Marks	50
Teaching Hours/Week (L:T:P:S)	1:2:0	SEE Marks	50
Credits	02	Exam Hours	02

Course objectives:

- To programming skills in Html5, CSS3, Bootstrap 4.
- To developing skills of Web Applications user interactions using JavaScript (i.e. ES6+).
- To design web application Development Database with React and React Native.
- To provide security for database and web application

Sl.NO	Experiments
1	HTML Layouts And Links: a.Develop a web application to control over different layouts. b. Create a webpage with HTML describing your department use paragraph and list tags. c. Apply various colors to suitable distinguish key words, also apply font styling like italics, underline and two other fonts to words you find appropriate, also use header tags.
2	Web Apllication Design Formtting: a. Develop a web application with background banner image and navigation menus. b. Develop a web application with responsive images. c. Develop a web application using left menu.
3	Introduction To Responsive Interface Using Bootsrap: Write code for developing responsive web application with Admin panel and tables with static data.
4	Chat Application API Responses: a. Context API Problem-solution for the chat messages. b. Denormalization of the data to be stored in app. c. Displaying chat feed for Interactive UI along with Real time user presence.
5	Programming With React: a. Basics Interactive examples. b. Function Components and Class Components c. React Native Fundamental, Handling Text Input, d. Using a scroll View, using List View. e. Platform Specific Code.
6	Databases Handling: a.Role Based Access. b. Messages Likes and deletion. c. File and Audio Chat Messages d. Extended Chat Features and Deployment
	Demonstration Experiments (For CIE) if any
7	Build A Drunken Snake Game Using Hooks a. Introduction and scaffolding the project. b. Components, Props and Styles. c. State and Lifecycle Events. d. Extended Game Functionality. e. Finishing up and Deployment.
8	Chat Application a. Firebase Environment. Introduction and Scaffolding the project. b. Private and Public pages, Context API. c. Creating Side bar and Dashboard d. Creating and displaying Chat Rooms. e. Creating Layout for Chat page.

Course outcomes (Course Skill Set):

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

- Designing a web page with using HTM, CSS, JavaScript.
- Use a Bootstrap to interface the web responsive.
- Develop the application for chat and design database.
- Provide security for database and web application

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

Suggested Learning Resources:

- https://www.infosecinstitute.com/skills/learning-paths/database-security/
- https://www.codecademy.com/learn/paths/web-development/
- https://nptel.ac.in/courses/106/105/106105084/
- https://medium.com/@aureliomerenda/create-a-native-web-app-with-react-native-web-419acac86b82
- https://www.coursera.org/learn/react-native
- https://desirecourse.net/react-native-and-redux-course-using-hooks/

REFERENCE BOOKS:

1. Adam Boduch and Roy Derks, "React and React Native: A Complete Hands-on Guide to Modern Web and Mobile Development with React.js", 3rd Edition, 2020.
2. W Hans Bergsten, "Java Server Pages", O'Reilly, 3rd Edition, 2003.
3. D.Flanagan,"Java Script", O'Reilly, 6th Edition, 2011.
4. Jon Duckett, "Beginning Web Programming", 2008.