Advances in Operating Systems			
Course Code	**MSCS201**	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	3

Course Learning objectives:

- Analyze the characteristics of operating systems for multiprocessor and multicomputer architectures.
- Understand and address the challenges related to designing operating systems.
- Explore the latest trends in developing mobile operating systems.
- Evaluate the implications of these trends on performance and user experience.

Module-1

Multiprocessor Operating Systems: System Architectures- Structures of OS – OS design issues – Process synchronization – Process Scheduling and Allocation- Memory Management.

Teaching- Learning Process	Chalk and talk/ Power point presentation/ Board

Module-2

Distributed Operating Systems: System Architectures- Design issues – Communication models – clock synchronization – mutual exclusion – election algorithms- Distributed Deadlock detection.

Teaching- Learning Process	Chalk and talk/ Power point presentation/ Board

Module-3

Distributed scheduling - Distributed shared memory - Distributed File system – Multimedia file systems - File placement – Caching.

Teaching- Learning Process	Chalk and talk/ Power point presentation/ Board

Module-4

Database Operating Systems: Requirements of Database OS – Transaction process model – Synchronization primitives - Concurrency control algorithms.

Teaching- Learning Process	Chalk and talk/ Power point presentation/ Board

Module-5

Mobile Operating Systems: ARM and Intel architectures - Power Management - Mobile OS Architectures - Underlying OS - Kernel structure and native level programming - Runtime issues- Approaches to power management.

Teaching- Learning Process	Chalk and talk/ Power point presentation/ Board

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:

- Two Unit Tests each of **25 Marks**
- Two assignments each of **25 Marks or one Skill Development Activity of 50 marks**

to attain the COs and POs

The sum of two 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. M Singhal and NG Shivaratri , Advanced Concepts in Operating Systems, Tata McGraw Hill Inc, 2001

Reference Book

1. A S Tanenbaum, Distributed Operating Systems, Pearson Education Asia, 2001
2. Source Wikipedia, Mobile Operating Systems, General Books LLC, 2010

Skill Development Activities Suggested

- Thestudentswiththehelpofthecourseteachercantakeuprelevanttechnical–activitieswhichwillenhancetheir 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	BloomsLevel
CO1	Analyze the characteristics of operating systems for multiprocessor and multicomputer architectures.	L2
CO2	Understand and address the challenges related to designing operating systems and their implications.	L3
CO3	Explore the latest trends in developing mobile operating systems and evaluate their impact on performance.	L4

Program Outcome of this course :

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

Mapping of COS and POs:

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

ETHICAL HACKING			
Course Code	**MSCR202**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	3:0:1	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	04	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/ Board

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/ Board

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/ Board

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/ Board

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/ Board

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:

- Two Unit Tests each of **25 Marks**
- Two assignments each of **25 Marks or one Skill Development Activity of 50 marks**

› attain the COs and POs

The sum of two 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.

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

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	PO5

	engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations	
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	MSCR203	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	3:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:

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

Module-1	
Blockchain 101: Distributed systems, History of blockchain, Introduction to blockchain, Types of blockchain, CAP theorem and blockchain, Benefits and limitations of blockchain.	
Teaching Learning Process	Chalk and talk/ Power point presentation/ Board

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/ Power point presentation/ Board

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/ Power point presentation/ Board

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/ Power point presentation/ Board

Module-5	
Alternative Blockchains: Blockchains Blockchain-Outside of Currencies: Internet of Things, Government, Health, Finance, Media	
Teaching-Learning Process	Chalk and talk/ Power point presentation/ Board

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:

- Two Unit Tests each of **25 Marks**
- Two assignments each of **25 Marks or one Skill Development Activity of 50 marks**

› attain the COs and POs

The sum of two 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:

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

Suggested Learning Resources:

Text Books:

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

Reference Books:

1. *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, Daniel Drescher, Apress, First Edition, 2017
2. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies,* Andreas M. Antonopoulos, O'Reilly Media, First Edition, 2014

Web links and Video Lectures (e-Resources):

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

Skill Development Activities Suggested

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

Course outcome (Course Skill Set)

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

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

Mapping of COS and POs

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

Program Outcome of this course

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

Defensive Security			
Course Code	**MSCR214A**	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 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/ Power point presentation/ Board

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/ Power point presentation/ Board

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/ Power point presentation/ Board

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/ Power point presentation/ Board

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/ Power point presentation/ Board

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:

- Two Unit Tests each of **25 Marks**
- Two assignments each of **25 Marks or one Skill Development Activity of 50 mark**

ɔ attain the COs and POs

The sum of two 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.

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.

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

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

Cyber threat Simulation Management

Course Code	MSCR214B	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 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/ Board

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/ Board

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/ Board

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/ Board

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/ Board

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:

- Two Unit Tests each of **25 Marks**
- Two assignments each of **25 Marks or one Skill Development Activity of 50 marks**

› attain the COs and POs

The sum of two 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:

- The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
- Each full question will have a sub-question covering all the topics under a module.
- 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**		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

CYBER SECURITY AND CYBER LAW			
Course Code	**MSCR214C**	CIE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	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/ PPT/ Board

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/ PPT/ Board

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/ PPT/ Board

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/ PPT/ Board

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/ PPT/ Board

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:

- Two Unit Tests each of **25 Marks**
- Two assignments each of **25 Marks or one Skill Development Activity of 50 marks**

ɔ attain the COs and POs

The sum of two 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

Data Protection **and Security**			
Course Code	MSCR214D	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:

- Define Data Protection
- Explain the information life cycle management
- Explore the role of Data retention
- Illustrate Confidentiality in Data Protection

Module-1

Business continuity: the first foundation for data protection ,Data Protection-Where the problem Lie ,Data Protection-,Setting the right Objectives ,data protection-Getting the right Degree

Teaching- Learning Process	Chalk and Talk/ PPT/ Board

Module-2

Information Life cycle management changes the data protection technology Mix, Compliance-A key piece of the GRC Puzzle

Teaching- Learning Process	Chalk and Talk/ PPT/ Board

Module-3

Governance : Data Governance must respond to changes in the federal rules of civil procedure, the impact of Global Civil litigation, the big 3 –governance, Risk management and compliance and data protection objectives. The critical role of Data retention: the need for data retention management, where the responsibility for data retention policy management lies, making the case for archiving for retention.

Teaching- Learning Process	Chalk and Talk/ PPT/ Board

Module-4

Data Security: How the Protection and data security are interrelated, Information security versus data security, Information assurance, Information risk management, Data Preservation is data that is good to the last bit, Confidentiality as a private and public concern, The role of data availability in data security, 3 strategies for protecting confidentiality of information , Confidentiality through limiting access to data , Confidentiality through limiting use of information, confidentiality by rendering information, the special case of storage security.

Teaching- Learning Process	Chalk and Talk/ PPT/ Board

Module-5

Cloud computing, SaaS and Other Data Protection Services; Growth in service raises questions for Protection, An Introduction to clod computing, Where IT services are headed, Data Protection Consideration in using a services model,

Teaching- Learning Process	Chalk and Talk/ PPT/ Board

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:

- Two Unit Tests each of **25 Marks**
- Two assignments each of **25 Marks or one Skill Development Activity of 50 marks**

to attain the COs and POs

The sum of two 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:

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

Suggested Learning Resources:

Books

1. Data Protection: Governance, Risk Management, and Compliance, By David G. Hill,2019

Reference Book

Data Privacy and Security ,David Salomon, Spring.2003

Web links and Video Lectures (e-Resources):

.**Web links and Video Lectures (e-Resources):**

https://youtu.be/Abta0j826Bk

- https://youtu.be/fQ3ESFfvchg?list=PLUtfVcb-iqn834VGI9faVXGIGSDXZMGp8

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Illustrate the basics of Data protection	L2
CO2	Define GRC Puzzle	L2
CO3	Explain the risk management and compliance and data protection objectives.	L2
CO4	Explore the relationship between Data Protection and data security	L2

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
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

SECURED PROGRAMMING			
Course Code	**MSCR215A**	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:

- 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/ PPT/ Board

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/ PPT/ Board

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/ PPT/ Board

Module-4

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

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:

- Two Unit Tests each of **25 Marks**
- Two assignments each of **25 Marks or one Skill Development Activity of 50 marks**

› attain the COs and POs

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

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

Semester End Examination:

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

Suggested Learning Resources:

Text Books

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

Reference Books

1. *Secure Programming for Linux and Unix HowTo David Wheeler Linux Documentation project* 2004.
2. *Secure Programming Cookbook for C and C++*, JohnViega, Matt Messier ,O'Reilly Media, 2003

Web links and Video Lectures (e-Resources):

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

Skill Development Activities Suggested

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

Course outcome (Course Skill Set)

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

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

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO 5	PO6	PO7	PO8	PO9	PO1 0	PO1 1	PO1 2
CO1	X											
CO2					**X**							
CO3				**X**			**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

BIOMETRIC SECURITY			
Course Code	**MSCR215B**	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:

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

Module-1

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

Teaching-Learning Process	Chalk and Talk/ PPT/ Board

Module-2

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

Teaching-Learning Process	Chalk and Talk/ PPT/ Board

Module-3

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

Teaching-Learning Process	Chalk and Talk/ PPT/ Board

Module-4

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

Teaching-Learning Process	Chalk and Talk/ PPT/ Board

Module-5

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

Teaching-Learning Process	Chalk and Talk/ PPT/ Board

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:

- Two Unit Tests each of **25 Marks**
- Two assignments each of **25 Marks or one Skill Development Activity of 50 marks**

ɔ attain the COs and POs

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

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

Semester End Examination:

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

Suggested Learning Resources:

Text Books

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

Reference Books

1. *Biometrics for Network Security* ,John Berger Prentice Hall 2004
2. *Implementing Biometric Security* ,John Chirillo and Scott Blaul ,Wiley, Eastern Publications 2005

Web links and Video Lectures (e-Resources):

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

Skill Development Activities Suggested

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

Course outcome (Course Skill Set)

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

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

Mapping of COS and POs

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

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	Po1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
3	Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.	PO3
4	Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.	PO4
5	Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations	PO5

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

ADVANCED CRYPTOGRAPHIC TECHNIQUES

Course Code	**MSCR215C**	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:

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

Module-1

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

Teaching-Learning Process	Chalk and Talk/ PPT/ Board

Module-2

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

Teaching-Learning Process	Chalk and Talk/ PPT/ Board

Module-3

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

Teaching-Learning Process	Chalk and Talk/ PPT/ Board

Module-4

Key Management and Distribution :Symmetric Key Distribution Using Symmetric Encryption Symmetric Key Distribution Using Asymmetric Encryption Distribution of Public Keys X.509 Certificates Public-Key Infrastructure , User Authentication Remote User-Authentication Principles Remote User-Authentication Using Symmetric Encryption Kerberos Remote User Authentication Using Asymmetric Encryption Federated Identity Management Personal Identity Verification 484

Teaching-Learning Process	Chalk and Talk/ PPT/ Board

Module-5

Transport-Level Security Web Security Considerations Secure Sockets Layer Transport Layer Security HTTPS Secure Shell (SSH) Wireless Security Wireless Network Threats Wireless Security Measures Mobile Device Security Security Threats Mobile Device Security Strategy Pretty Good Privacy Notation Operational Description S/MIME RFC 5322 Multipurpose Internet Mail Extensions S/MIME Functionality S/MIME Messages S/MIME Certificate Processing Enhanced Security Services

Teaching-Learning Process	Chalk and Talk/ PPT/ Board

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:

- Two Unit Tests each of **25 Marks**
- Two assignments each of **25 Marks or one Skill Development Activity of 50 marks**

ɔ attain the COs and POs

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

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

Semester End Examination:

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

Suggested Learning Resources:

Books

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

Web links and Video Lectures (e-Resources):

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

Skill Development Activities Suggested

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

Course outcome (Course Skill Set)

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

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

Mapping of COS and POs

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

Program Outcomes

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	Po1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
3	Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.	PO3

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

FILE SYSTEM FORENSIC ANALYSIS			
Course Code	**MSCR215D**	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:

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

Module-1

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

Teaching-Learning Process	Chalk and Talk/ PPT/ Board

Module-2

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

Teaching-Learning Process	Chalk and Talk/ PPT/ Board

Module-3

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

Teaching-Learning Process	Chalk and Talk/ PPT/ Board

Module-4

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

Teaching-Learning Process	Chalk and Talk/ PPT/ Board

Module-5

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

Teaching-Learning Process	Chalk and Talk/ PPT/ Board

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:

- Two Unit Tests each of **25 Marks**
- Two assignments each of **25 Marks or one Skill Development Activity of 50 marks**

ɔ attain the COs and POs

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

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

Semester End Examination:

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

Suggested Learning Resources:

Text Books

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

Reference Books

1. Introduction to Linux A Hands-On Guide, MachteltGarrels, Fultus CorporationPublisher, Third Edition 2010.
2. Computer Forensics, Warren and Jay Heiser, Kruse, Addison Wesley, 2002.
3. Guide to Computer Forensics and Investigations, Bill Nelson, Amelia Phillips, Frank Enfinger, Chris Steuart, Thomson Course Technology, 2004
4. Forensic Discovery, Dan Farmer & WietseVenema, Addison Wesley, 2005

Web links and Video Lectures (e-Resources):

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

Skill Development Activities Suggested

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

Course outcome (Course Skill Set)

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

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

Mapping of COS and POs

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

Program Outcome of this course

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

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

ETHICAL HACKING LABORATORY			
Course Code	**MSCRL207**	CIE Marks	50
Teaching Hours/Week (L:T:P: S)	0:2:0	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 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

Mini Project with Seminar			
Course Code	MSCR206	CIE Marks	50
Number of Contact Hours/Week	2	SEE Marks	**50**
Credits	03	Exam Hours	**03**

Course objectives:

- To support independent learning and innovative attitude.
- To guide to select and utilize adequate information from varied resources upholding ethics.
- To guide to organize the work in the appropriate manner and present information (acknowledging the sources) clearly.
- To develop interactive, communication, organization, time management, and presentation skills.
- To impart flexibility and adaptability.
- To inspire independent and team working.
- To expand intellectual capacity, credibility, judgement, intuition.
- To adhere to punctuality, setting and meeting deadlines.
- To instill responsibilities to oneself and others.
- To train students to present the topic of project work in a seminar without any fear, face audience confidently, enhance communication skill, involve in group discussion to present and exchange ideas.

Mini-Project: Each student of the project batch shall involve in carrying out the project work jointly in constant consultation with internal guide, co-guide, and external guide and prepare the project report as per the norms avoiding plagiarism.

Course outcomes:

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

- Present the mini-project and be able to defend it.
- Make links across different areas of knowledge and to generate, develop and evaluate ideas and information so as to apply these skills to the project task.
- Habituated to critical thinking and use problem solving skills.
- Communicate effectively and to present ideas clearly and coherently in both the written and oral forms.
- Work in a team to achieve common goal.
- Learn on their own, reflect on their learning and take appropriate actions to improve it.

CIE procedure for Mini - Project:

The CIE marks awarded for Mini - Project, shall be based on the evaluation of Mini - Project Report, Project Presentation skill and Question and Answer session in the ratio 50:25:25.The marks awarded for Mini - Project report shall be the same for all the batch mates.

Semester End Examination

SEE marks for the mini-project shall be awarded based on the evaluation of Mini-Project Report, Presentation skill and Question and Answer session in the ratio 50:25:25 by the examiners appointed by the University.

SKILL ENHANCEMENT FOR RESEARCH EXCELLENCE-1			
Course Code	MSCS258	CIE Marks	50
Number of contact Hours/Week	2	SEE Marks	50
Credits	01	Exam Hours/Batch	03

The M.Tech Research Skills Development program equips students with essential skills for successful research and publication, including understanding research fundamentals, conducting literature reviews, selecting appropriate methodologies, writing proposals and papers, analyzing data, presenting findings, adhering to ethical standards, and engaging in networking and collaboration, culminating in the effective publication of only 1 research article to Scopus-indexed conferences.

Course objectives:

To produce high-quality research papers that meet the standards of international conferences or peer-reviewed journals.

To effectively identify suitable journals for publication based on the scope and impact of research findings.

To demonstrate proficiency in writing and structuring research papers according to academic conventions.

To engage in the peer review process, providing and receiving constructive feedback to enhance research quality.

To develop skills for presenting research at conferences, including crafting effective abstracts and posters.

To cultivate a strong understanding of ethical considerations in research and publication practices.

To utilize citation management tools to organize references and ensure proper attribution in publications.

To enhance collaboration skills for co-authoring papers and working within research teams.

To stay informed about current trends and advancements in the field to ensure relevance in publications.

To refine the ability to respond to reviewer comments and revise manuscripts effectively.

To understand the importance of open access and alternative publication models in disseminating research.

To build a professional network that supports research collaborations and publication opportunities.

Guidelines for Research paper preparation: Each student in a group of two members shall actively participate in carrying out the research work jointly, in constant consultation with the internal guide, mentors or co-guide, and external guide. They must prepare the project report as per the prescribed norms while ensuring plagiarism is avoided. A research group can have a maximum of two members.

Understanding Research Fundamentals

Definition of Research: Understand what constitutes research and its significance in technology and engineering.

Types of Research:

Basic Research: Focused on gaining comprehensive knowledge without immediate applications.

Applied Research: Aimed at solving specific problems.

Literature Review

Conducting a Literature Survey:

Identify relevant academic papers, journals, and conference proceedings.

Summarize key findings and methodologies from existing literature.

Critical Analysis:

Evaluate the strengths and weaknesses of existing research.

Identify gaps in the literature that your research can address.

Research Methodology

Selecting a Research Topic:

Choose a topic that aligns with your interests and current trends in technology.

Research Design:

Decide on qualitative, quantitative, or mixed methods based on your research objectives.

Data Collection Techniques:

Surveys, interviews, experiments, and simulations.

Writing Research Proposals

Structure of a Proposal:

Introduction, Literature Review, Methodology, Expected Outcomes, and References.

Proposal Presentation:

Practice presenting your proposal to peers and faculty for feedback.

Data Analysis

Statistical Tools:

Familiarize yourself with tools like MATLAB, R, or Python for data analysis.

Interpreting Results:

Learn to draw meaningful conclusions from your data and relate them back to your research questions.

Writing Research Papers

Structure of a Research Paper:

Abstract, Introduction, Methodology, Results, Discussion, Conclusion, and References.

Academic Writing Skills:

Focus on clarity, coherence, and proper citation of sources.

Peer Review Process:

Understand the importance of peer review and how to respond to reviewers' comments.

Presentation Skills

Effective Communication:

Develop skills to present your research findings clearly and confidently.

Use of Visual Aids:

Incorporate slides, charts, and graphs to enhance your presentations.

Ethical Considerations in Research

Understanding Ethics:

Familiarize yourself with ethical guidelines related to research involving human subjects, data privacy, and plagiarism.

Responsible Conduct of Research:

Promote integrity and accountability in your research practices.

Submitting Manuscripts to Scopus-Indexed Conferences or Web of Science or Proceedings /Book Chapters

Identify Relevant Conferences

Research Scopus-Indexed Conferences:

Use platforms like Conference Alerts, IEEE Xplore, or the Scopus website to find conferences in your field.

Check Conference Indexing:

Ensure that the conference is indexed in Scopus by checking its official website or the Scopus database.

Prepare Your Manuscript

Follow Conference Guidelines:

Each conference has specific formatting and submission guidelines. Adhere to these requirements.

Structure of the Manuscript:

Title, Abstract, Introduction, Methodology, Results, Discussion, Conclusion, and References.

Language and Clarity:

Use clear and concise language. Consider having your manuscript proofread by peers or professionals.

Submission of manuscript, Registration and Presentation finally Publication

Course outcomes:

- At the end of the course the student will be able to:
- Produce High-Quality Research Papers: Create research papers that meet international conference and peer-reviewed journal standards.
- Identify Suitable Journals: Effectively select appropriate journals for publication based on research scope and impact.
- Proficiency in Writing: Demonstrate skill in writing and structuring research papers according to academic conventions.
- Engage in Peer Review: Actively participate in the peer review process by providing and receiving constructive feedback.
- Develop Presentation Skills: Acquire skills for presenting research at conferences, including crafting effective abstracts and posters.
- Understand Ethical Considerations: Cultivate a strong understanding of ethical issues in research and publication practices.
- Utilize Citation Management Tools: Use citation management tools to organize references and ensure proper attribution.
- Respond to Reviewer Comments: Refine the ability to address reviewer comments and revise manuscripts effectively.

The assessment for **Skill Enhancement for Research Excellence** will be divided into **Continuous Internal Evaluation (CIE) and Semester End Examination (SEE), each carrying 50 marks.**

Continuous Internal Evaluation (CIE) – 50 Marks

CIE shall be conducted **weekly** and will be assessed based on:

- **Base Papers Referred & Review** – 10 Marks
- **Presentations on Proposed Concepts** – 15 Marks
- **Preparation of Conference Papers (Preferably Scopus Indexed or Reputed Conferences)** – 25 Marks

Semester End Examination (SEE) – 50 Marks

- The **SEE examiner may be appointed from the same college** for evaluation.
- The candidate must **present their research work** before the examiner.
- **Mandatory requirement:** The candidate must have **submitted a paper to a conference** or **accepted or presented** at a reputed conference.
- Marks will be awarded based on:
    - **Research Presentation Quality** – 25 Marks
    - **Clarity of Concept & Methodology** – 15 Marks
    - **Conference Submission & Acceptance/Presentation** – 10 Marks