Semester- III

	Anroid Forensics			
	Course Code	22SFC31	CIE Marks	50
	Teaching Hours/Week (L:P:SDA)	3:0:2	SEE Marks	50
	Total Hours of Pedagogy	40	Total Marks	100
	Credits	03	Exam Hours	03
	Course Learning objectives: ● Define the basics of Anroid and mobile forensics. ● Explore hardware requirements of Anroid devices ● Demonstrate , Android security model, Forensics and the SDK			
	Module-1			
	Android and mobile forensics: Introduction, Android platform, Linux, Open source software and forensics, Android Open Source Project, Internationalization, Android Market, Android forensics			
	Teaching-Learning Process	**Chalk and talk/PowerPoint presentation.**		
	Module-2			
	Android hardware platforms: Overview of core components, Overview of different device types, Readonly memory and boot loaders, Manufacturers, Specific devices.			
	Teaching-Learning Process	**Chalk and talk/PowerPoint presentation.**		
	Module-3			
	Android software development kit and android debug bridge: Android platforms, Software development kit (SDK), Android security model, Forensics and the SDK.			
	Teaching-Learning Process	**Chalk and talk/PowerPoint presentation.**		
	Module-4			
	Android file systems and data structures: Data in the shell, Type of memory, File systems, Mounted file systems and directory structures. Android forensic techniques: Procedures for handling an Android device, Imaging Android USB mass storage devices, Logical techniques, Physical techniques.			
	Teaching-Learning Process	**Chalk and talk/PowerPoint presentation.**		
	Module-5			
	Android device data and app security: Data theft targets and attack vectors, Security considerations, Individual security strategies, Corporate security strategies, App development security strategies. Android application and forensic analysis: Analysis techniques, FAT forensic analysis, YAFFS2 forensic analysis, Android app analysis.			
	Teaching-Learning Process	**Chalk and talk/PowerPoint presentation.**		

Assessment Details (both CIE and SEE)

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

Continuous Internal Evaluation:

- Three Unit Tests each of **20 Marks**
- Two assignments each of **20 Marks** or **one Skill Development Activity of 40 marks**

to attain the COs and POs

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

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

Semester End Examination:

- 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:

Books

- *Android Forensics Investigation, Analysis, and Mobile security for Google Android* , Andrew Hoog, John McCash, , Technical Editor, Elsevier

Reference Book

1. *Practical Mobile Forensics,* SatishBommisetty, RohitTamma, Heather Mahalik, Packt Publishing,2014
2. *Mobile Device Forensics,* Andrew Martin, SANS Institute, 2009

- **Web links and Video Lectures (e-Resources):**
  https://youtu.be/5e5KdbY-xzE
  https://youtu.be/BSr7Giw3roo
  https://youtu.be/PW8-TGGAE3o

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Demonstrate security risks and vulnerabilities from mobile devices and network access.	L3
CO2	Explain the methods and procedures used in forensics investigations	L3
CO3	Explore the knowledge of the global security threats and vulnerabilities of mobile devices and networks.	L2
Co4	Apply forensics investigation of mobile and network devices in real life.	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			x				x			

Semester- III

Security Architecture Design			
Course Code	22SFC321	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 the architecture Patterns in Security and software process.
- Explore Security and Perl, Bytecode Verification in Java-Good Coding.
- Demonstrate Mid-Level Architecture.

Module-1	
Architecture and Security: Architecture Reviews, Software Process, Reviews and the Software Development Cycle, Software Process and Architecture Models, Software Process and Security, Architecture Review of System, Security Assessments, Security Architecture Basics, Architecture Patterns in Security	
Teaching-Learning Process	**Chalk and talk/PowerPoint presentation.**

Module-2	
Low-Level Architecture: Code Review, importance of code review, Buffer Overflow Exploits, Countermeasures Against Buffer Overflow Attacks, patterns applicable, Security and Perl, Bytecode Verification in Java-Good Coding Practices Lead to Secure Code, Cryptography, Trusted Code, Secure Communications	
Teaching-Learning Process	**Chalk and talk/PowerPoint presentation.**

Module-3	
Mid-Level Architecture: Middleware Security, Middleware and Security, The Assumption of Infallibility, The Common Object Request Broker Architecture, The OMG CORBA Security Standard, Vendor Implementations of CORBA Security, CORBA Security Levels, Secure Interoperability, Application, Unaware Security, Application, Aware Security, Application Implications, Web Security, Application and OS Security, Database Security	
Teaching-Learning Process	**Chalk and talk/PowerPoint presentation.**

Module-4	
High-Level Architecture: Security Components, Secure Single Sign-On- Public-Key Infrastructures, Firewalls, Intrusion Detection Systems, LDAP and X.500 Directories, Kerberos, Distributed Computing Environment, The Secure Shell, or SSH, The Distributed Sandbox, Security and Other Architectural Goals, Metrics for Non-Functional Goals, Force Diagrams around Security, High Availability, Robustness, Reconstruction of Events, Ease of Use, Maintainability, Adaptability, and Evolution, Scalability, Interoperability, Performance, Portability.	
Teaching-Learning Process	**Chalk and talk/PowerPoint presentation.**

Module-5

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

Assessment Details (both CIE and SEE)

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

Continuous Internal Evaluation:

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

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

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

Semester End Examination:

- 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:

Books

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

Reference Book

2. *Security Patterns: Integrating Security and Systems Engineering* Markus Schumacher Wiley Software Pattern Series 2010

Web links and Video Lectures (e-Resources):

https://youtu.be/voMhlWZvpPE
https://youtu.be/LREcVbHiqTo

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Design the secured sites based on tools & techniques and CORBA Security	L3
CO2	Demonstrate the working of High-Level security Architecture	L3
CO3	Identify Enterprise Security Architecture	L2

Mapping of COS and POs

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

Semester- III

Steganography and Digital Watermarking			
Course Code	22SFC322	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 Information hiding and Steganography systems.
- Interpret Steganalysis techniques
- Explore watermarking techniques

Module-1

Introduction to Information hiding: Brief history and applications of information hiding, Principles of Steganography, Frameworks for secret communication, Security of Steganography systems, Information hiding in noisy data, Adaptive versus non adaptive algorithms, Laplace filtering, Using cover models, Active and malicious attackers, Information hiding in written text, Examples of invisible communications.

Teaching-Learning Process	**Chalk and talk/PowerPoint presentation.**

Module-2

Survey of steganographic techniques: Substitution system and bit plane tools, Transform domain techniques, Spread spectrum and information hiding, Statistical Steganography, Distortion and code generation techniques, Automated generation of English text.

Teaching-Learning Process	**Chalk and talk/PowerPoint presentation.**

Module-3

Steganalysis: Detecting hidden information, Extracting hidden information, Disabling hidden information, Watermarking techniques, History, Basic Principles, applications, Requirements of algorithmic design issues, Evaluation and benchmarking of watermarking system.

Teaching-Learning Process	**Chalk and talk/PowerPoint presentation.**

Module-4

Survey of current watermarking techniques: Cryptographic and psycho visual aspects, Choice of a workspace, binary image, audio, video. Formatting the watermark beds: Digital watermarking schemes, Spread Spectrum, DCT (Discrete Cosine Transform), Domain and Quantization schemes, Watermarking with side information, Robustness to temporal and geometric distortions.

Teaching-Learning Process	**Chalk and talk/PowerPoint presentation.**

Module-5

Data Right Management: DRM Products and Laws, Fingerprints, Examples, Protocols and Codes, BonehShaw finger printing Scheme, Steganography and watermarking applications, Military, Digital copyright protection and protection of intellectual property.

Teaching-Learning	**Chalk and talk/PowerPoint presentation.**

	Process	

Assessment Details (both CIE and SEE)

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

Continuous Internal Evaluation:

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

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

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

Semester End Examination:

- 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:

Books

- Information hiding techniques for Steganography and Digital Watermarking Stefan Katzenbelsser and Fabien A. P. Petitcolas ARTECH House
- Digital Water Marking and Steganography I.J. Cox, M.L. Miller, J.Fridrich and T.Kalker Morgan Kauffman 2nd
- Information Hiding: Steganography and Watermarking -Attacks and Countermeasures Johnson, Neil F. / Duric, Zoran / Jajodia, Sushil G Advances in Information Security

Reference Book

1. Disappearing Cryptography: Information Hiding, Steganography and Watermarking Peter Wayner Elsevier

Web links and Video Lectures (e-Resources):

https://youtu.be/habrsC934-4

https://youtu.be/habrsC934-4

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Distinguish steganography & Digital watermarking from other related fields	L3
CO2	Knowledge of how to use steganography techniques in conjunction with encryption systems to protect data.	L3
CO3	Explain different types of watermarking applications and watermarking frameworks.	L2
Co4	Explore Cryptographic and psycho visual aspects	L2
CO5	Explain Data Right Management concept.	L2

Mapping of COS and POs

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

Semester- III

	Network Security Monitoring			
	Course Code	22SFC323	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 Network Security Monitoring Rations ● Explore network traffic ● Learn NSM deployment and installation			
	Module-1			
	Network Security Monitoring Rations: An Introduction to NSM,A sample NSM Test, The range of NSM Data, NSM drawback,			
	Teaching-Learning Process	**Chalk and talk/PowerPoint presentation.**		
	Module-2			
	Collecting network traffic: Access,Storage and management: A sample Network for apilot NSM system, IP address and network address Translation,Choosing the best plce to obtain Network visibility,Getting physical Access to the Traffic,chossong an NSM Platform.			
	Teaching-Learning Process	**Chalk and talk/PowerPoint presentation.**		
	Module-3			
	Stand alone NSM deployment and installation: Stand alone or server plus sensors,Choosing how to get SO Code onto hardware,installing a stand alone system, Distributed deployment:installing an SO server using the SO .iso image,installing an SO sensor using the SO .iso image,Building an SO server using PPAs,Building an SO sensor using PPAs.			
	Teaching-Learning Process	**Chalk and talk/PowerPoint presentation.**		
	Module-4			
	Command Line packet analysis tools: SO tool Categories,Running Tcpdump,Using Dumpcap and Tshark,Running Argus and the Ra Client,Graphical Packet analysis tools: usinh Wireshark,Using Xplico,NSM Consoles:An NSM centric look at network Traffic,Using Sguil,Uisng Squert,Using Snorby,Using ELSA.			
	Teaching-Learning Process	**Chalk and talk/PowerPoint presentation.**		
	Module-5			
	NSM Operations: The Enterprise Security Cycle ,Collection,Analysis,Esaclation and Resolution, Server side Compromise Defined, server Side Compromise: Server side compromise defined, action, Exploring the session data, steeping back			
	Teaching-Learning	**Chalk and talk/PowerPoint presentation.**		

	Process	

Assessment Details (both CIE and SEE)

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

Continuous Internal Evaluation:

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

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

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

Semester End Examination:

- 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:

Books

1. The Practice of Network security monitoring:understanding incident detection and response ,Richard Bejtlich,No starch press,san Francisco.

Reference Book

2. Applied Network Security Monitoring: Collection, Detection, and Analysis, Chris Sanders, Jason Smith, Syngress; 1st edition (December 19, 2013)

Web links and Video Lectures (e-Resources):

https://youtu.be/oouR87i5r9c
https://youtu.be/ubQxWUCtzpw

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Build an SO sensor using PPAs	L3
CO2	Demonstrate the working of SO server using the SO .iso image,	L3
CO3	Demonstrate Command Line packet analysis using tools	L2
Co4	Explore Server side compromise	L2

Mapping of COS and POs

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

Semester- III

	Security Assessment and Verification			
	Course Code	22SFC324	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 the Evolution of information security
- Illustrate the Security Assessment
- Explain Risk Analysis

	Module-1	
	Evolution of information security: information assets, security standards, organizational impacts, security certifications, elements of information security program, need for security assessment, security assessment process.	
	Teaching-Learning Process	**Chalk and talk/PowerPoint presentation.**
	Module-2	
	Security assessment planning: Business drivers, scope definition, consultant's perspective, Client's perspective, Development of project plan. Initial information gathering, Initial preparation, analysis of gathered information	
	Teaching-Learning Process	**Chalk and talk/PowerPoint presentation.**
	Module-3	
	Business process evaluation, Technology evaluation, Risk analysis, Risk mitigation.	
	Teaching-Learning Process	**Chalk and talk/PowerPoint presentation.**
	Module-4	
	Security Risk assessment project management, Security risk assessment approaches and methods	
	Teaching-Learning Process	**Chalk and talk/PowerPoint presentation.**
	Module-5	
	Information security standards, Information security Legislation, Formal security verification, Security verification with SSL.	
	Teaching-Learning Process	**Chalk and talk/PowerPoint presentation.**

Assessment Details (both CIE and SEE)

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

Continuous Internal Evaluation:

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

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

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

Semester End Examination:

- 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:

Books

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

Reference Book

- Principles of Information Security Michael E. Whitman, Herbert J. Mattord Cengage Learning 2nd Edition
- Information Security Fundamentals Thomas R Peltier, Justin Peltier and John Blackley Prentice Hall 2nd Edition, 1996

Web links and Video Lectures (e-Resources):

https://youtu.be/61JFiAtViUY
https://youtu.be/_s6qDjgCbCE

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 roles information security and its management	L3
CO2	Select appropriate techniques to tackle and solve problems in the discipline of information security assessment	L3
CO3	Design an information security and validation system	L2

Mapping of COS and POs

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

Semester- III

	Data Protection and Security			
	Course Code	22SFC325	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/PowerPoint presentation.**
	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/PowerPoint presentation.**
	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 data retention.	
	Teaching-Learning Process	**Chalk and talk/PowerPoint presentation.**
	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/PowerPoint presentation.**
	Module-5	
	Cloud computing, SaaS and Other Data Protection Services; Growth in service raises questions for data 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/PowerPoint presentation.**

Assessment Details (both CIE and SEE)

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

Continuous Internal Evaluation:

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

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

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

Semester End Examination:

- 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:

Books

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

Reference Book

2. Data Privacy and Security ,David Salomon, Spring.2003

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
CO5	Demonstrate the Data protection Cloud	L2

Mapping of COS and POs

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

Semester- III

	NETWORK AND CLOUD SECURITY			
	Course Code	22SFC331	CIE Marks	50
	Teaching Hours/Week (L:P:SDA)	3:0:0	SEE Marks	50
	Total Hours of Pedagogy	40	Total Marks	100
	Credits	04	Exam Hours	03

Course Learning objectives:

- To define the Security associated with computer networks.
- To describe various communications networks and their main components.
- To identify the benefits and characteristics of cloud computing.
- To describe the various virtualization techniques and vulnerabilities.

Module-1

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

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

Module-2

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

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

Module-3

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

Assessment Details (both CIE and SEE)

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

Continuous Internal Evaluation:

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

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

Semester End Examination:

- 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

Text Books:

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

Reference Books:

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

Web links and Video Lectures (e-Resources):

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

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms L
CO1	Identify the security issues in the network and resolve it.	L1
CO2	Illustrate the different types of cloud solutions among IaaS, PaaS, SaaS.	L3

CO3	Define the recommendations for using and managing the customer's identity and choose the type of virtualization to be used	L1
CO4	Analyze the vulnerabilities in any computing system and hence be able to choose a security solution.	L4(through Assignment)

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

Mapping of COS and POs

	ETHICAL HACKING			
	Course Code	22SFC332	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:

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

Module-1

Introduction to ethical hacking: Fundamentals of computer networking. TCP/IP protocol stacks.

Casing the Establishment**:** What is foot printing, Internet Foot printing, Scanning, Enumeration, basic banner grabbing, Enumerating Common Network services. Case study: Network Security Monitoring.

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

Module-2

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

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

Module-3

Dial-up, PBX, Voicemail and VPN hacking, Preparing to dial up, War-Dialing, Brute-Force Scripting PBX hacking, Voice mail hacking, VPN hacking, Network Devices: Discovery Autonomous System Lookup, Public Newsgroups, Service Detection, Network Vulnerability, Detecting Layer 2 Media.

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

Module-4

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

Teaching-Learning Process	Chalk and talk/Power point presentation/ Show the Tool usage for foot printing/ Assignment: write an article about Firewall

Module-5

Remote Control Insecurities: Discovering Remote Control Software, Connection, Weakness.VNC, Microsoft Terminal Server and Citrix ICA, Advanced Techniques Session Hijacking, Back Doors, Trojans, Cryptography, Subverting the systems Environment, Social Engineering, Web Hacking, Web server hacking web application hacking, Hacking the internet Use, Malicious Mobile code, SSL fraud, E-mail Hacking, IRC hacking, Global countermeasures to Internet User Hacking.

Teaching-Learning Process	Chalk and talk/ Power point presentation Classroom Interaction/ Web resources.

Assessment Details (both CIE and SEE)

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

Continuous Internal Evaluation:

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

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

Semester End Examination:

- 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:

Text Books

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

Reference Books

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

Web links and Video Lectures (e-Resources):

- https://www.simplilearn.com/cyber-security/ceh-certification?utm_source=google&utm_medium=cpc&utm_term=&utm_content=1632205197-79872225071-377654317159&utm_device=c&utm_campaign=Search-TechCluster-Cyber-OthersNew-IN-Main-AllDevice-adgroup-DSA-Category-

Page&gclid=CjwKCAjwg5uZBhATEiwAhhRLHpJKcI-8Jzytg1p9ByQBrSs1Pc5R0GcklMm-sGq3foLJah3xJ0z3lhoCSPMQAvD_BwE.

- https://hackr.io/blog/best-ethical-hacking-courses
- https://www.udemy.com/topic/ethical-hacking
- https://onlinecourses.nptel.ac.in/noc19_cs68/preview

Skill Development Activities 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 Le
CO1	Identify the AI based problems	L1
CO2	Discuss on expert systems	L2
CO3	Apply techniques to solve the AI problems	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									

Semester- III

	Cyber threat Simulation Management			
	Course Code	2SFC333	CIE Marks	50
	Teaching Hours/Week (L:P:SDA)	2:0:2	SEE Marks	50
	Total Hours of Pedagogy	40	Total Marks	100
	Credits	03	Exam Hours	03

Course Learning objectives:

- To identify different types of threats for management.
- To recognize the vulnerability in the digital society.
- To use trends and identifying the risk councils and worst occurs.

Module-1	
The Cyber Threat to the Corporate Brand: The Rise of Cyber Organized Crime and Its Global Impact, Is Nothing Sacred? The Liberty Reserve Case: Money Laundering in the Digital Age, The Corruption Factor, Information Threat, Physical Threat, The Emergence of the Cyber Nation-State and Technology Espionage, A Case of Cyber Espionage Conspiracy? According to the Select Committee…	
Teaching-Learning Process	Chalk and Talk/ PPT/ Web Resources https://www.youtube.com/watch?v=WRIakA5CP3I

Module-2	
Corporate Vulnerabilities in the Digital Society: What Is the True Cost of a Cyber Attack? Cyber Attack Detection Sometimes Takes Years, One of the First Questions: "How Much Will This Cost?"A Few Common Cost Factors, What About Unreported Breaches? Cyber Attacks Result in a Wider Impact: The Community, U.S. Cyber Public Policy, No Guarantees with this Executive Order, Government-Industry Cooperation: No Silver Bullet, The Challenge of Defining Cyber Public Policy, Cold War II: The Cyber Chapter, Is There a Silver Lining in an Attack?	
Teaching-Learning Process	Chalk and Talk/ PPT/ Assignment

Module-3	
Four Trends Driving Cyber Breaches and Increasing Corporate Risk: Technology Trend, Loss of Situational Awareness: Distraction, Culture, Technology is a Double-Edged Sword, Social Media and Digital Protest, Social Media: A Tool for Disruption, a Model for Change, The Hacker Group Anonymous, Anarchaos: In the Image of Anonymous.	
Teaching-Learning Process	Chalk and Talk/ PPT/Seminar

Module-4	
Managing the Brand When the Worst Occurs: Be Prepared, Managing the Big Risk, Background Investigation Suggestions to Improve Process, Risk-Reinforced Service Level Agreements, Clouds Fill the Horizon.	
Teaching-Learning Process	Chalk and Talk/ PPT/Article

Module-5

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

Assessment Details (both CIE and SEE)

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

Continuous Internal Evaluation:

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

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

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

Semester End Examination:

- 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									
CO3				x								

Semester- III

Secured Programming			
Course Code	22SFC334	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 method /PPT/**

Module-2

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

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

Module-3

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

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

Module-4

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

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

Module-5

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

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

Assessment Details (both CIE and SEE)

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

Continuous Internal Evaluation:

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

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

Semester End Examination:

- 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.

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

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

Web links and Video Lectures (e-Resources):

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

Skill Development Activities Suggested

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

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Explain how to respond the security alerts which identifies software issues	L1
CO2	Identify possible security programming errors	L2
CO3	Define methodology for security testing and use appropriate tools in its implementation	L2
CO4	Apply new security-enhanced programming models and tools(can be attained through assignment or CIE)	L3

Mapping of COS and POs

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

Semester- III

	Deep Learning			
	Course Code	22SFC335	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 identify the context of neural networks and deep learning.
- To recognise how to use a neural network.
- To summarize the data needs of deep learning.
- To explore the working knowledge and the parameters of neural networks and deep learning.

MODULE-1	
Machine Learning Basics: Learning Algorithms, Capacity, Over fitting and Under fitting, Hyper parameters and Validation Sets, Estimator, Bias and Variance, Maximum Likelihood Estimation, Bayesian Statistics, Supervised Learning Algorithms, Unsupervised Learning Algorithms, Stochastic Gradient Descent, building a Machine Learning Algorithm, Challenges Motivating Deep Learning.	
Teaching-Learning Process	Chalk and board and PPT/web resources: https://www.youtube.com/watch?v=NOJOYcmyDhM
MODULE-2	
Deep Feed forward Networks: Gradient-Based Learning, Hidden Units, Architecture Design, Back Propagation. Regularization: Parameter Norm Penalties, Norm Penalties as Constrained Optimization, Regularization and Under-Constrained Problems, Dataset Augmentation, Noise Robustness, Semi Supervised Learning, Multi-Task Learning, Early Stopping, Parameter Tying and Parameter Sharing, Sparse Representations, Bagging, Dropout.	
Teaching-Learning Process	Chalk and board and PPT/Assignment
MODULE-3	
Optimization for Training Deep Models: How Learning Differs from Pure Optimization, Challenges in Neural Network Optimization, Basic Algorithms. Parameter Initialization Strategies, Algorithms with Adaptive Learning Rates. **Convolutional Networks:** The Convolution Operation, Motivation, Pooling, Convolution and Pooling as an Infinitely Strong Prior, Variants of the Basic Convolution Function, Structured Outputs, Data Types, Efficient Convolution Algorithms, Random or Unsupervised Features.	
Teaching-Learning Process	Chalk and board and PPT/ web resources: https://www.youtube.com/watch?v=zfiSAzpy9NM
MODULE-4	
Sequence Modelling: Recurrent and Recursive Nets: Unfolding Computational Graphs, Recurrent Neural Networks, Bidirectional RNNs, Encoder-Decoder Sequence-to-Sequence Architectures, Deep Recurrent Networks, Recursive Neural Networks. Long short-term memory	
Teaching-Learning Process	Chalk and board and PPT/Seminar

MODULE 5	
Practical Methodology: Performance Metrics, Default Baseline Models, Determining Whether to Gather More Data, Selecting Hyperparameters, Debugging Strategies, Example: Multi-Digit Number Recognition. Applications: Vision, NLP, Speech.	
Teaching-Learning Process	Chalk and board and PPT/Article/Assignment

Assessment Details (both CIE and SEE)

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

Continuous Internal Evaluation:

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

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

Semester End Examination:

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

Suggested Learning Resources:

TextBooks:

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

Reference books:

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

Web links and Video Lectures (e-Resources):

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

Skill Development Activities Suggested

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

Course outcome (Course Skill Set)

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

Sl. No.	Description	Blooms Level
CO1	Identify the deep learning algorithms which are more appropriate for various types of learning tasks in various domains.	L1
CO2	Implement deep learning algorithms and solve real-world problems.	L4
CO3	Execute performance metrics of Deep Learning Techniques.	L4

COs and POs Mapping:

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

PROJECT WORK PHASE - 1			
Course Code	22SFC34	CIE Marks	100
Number of contact Hours/Week	6	SEE Marks	--
Credits	03	Exam Hours	--

Course objectives:

- Support independent learning.
- Guide to select and utilize adequate information from varied resources maintaining ethics.
- Guide to organize the work in the appropriate manner and present information (acknowledging the sources) clearly.
- Develop interactive, communication, organisation, time management, and presentation skills.
- Impart flexibility and adaptability.
- Inspire independent and team working.
- Expand intellectual capacity, credibility, judgement, intuition.
- Adhere to punctuality, setting and meeting deadlines.
- Instil responsibilities to oneself and others.
- 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.

Project Phase-1 Students in consultation with the guide/s shall carry out literature survey/ visit industries to finalize the topic of the Project. Subsequently, the students shall collect the material required for the selected project, prepare synopsis and narrate the methodology to carry out the project work.

Seminar: Each student, under the guidance of a Faculty, is required to

- Present the seminar on the selected project orally and/or through power point slides.
- Answer the queries and involve in debate/discussion.
- Submit two copies of the typed report with a list of references.

The participants shall take part in discussion to foster friendly and stimulating environment in which the students are motivated to reach high standards and become self-confident.

Course outcomes:

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

- Demonstrate a sound technical knowledge of their selected project topic.
- Undertake problem identification, formulation, and solution.
- Design engineering solutions to complex problems utilising a systems approach.
- Communicate with engineers and the community at large in written an oral forms.
- Demonstrate the knowledge, skills and attitudes of a professional engineer.

Continuous Internal Evaluation

CIE marks for the project report (50 marks), seminar (30 marks) and question and answer (20 marks) shall be awarded (based on the quality of report and presentation skill, participation in the question and answer session by the student) by the committee constituted for the purpose by the Head of the Department. The committee shall consist of three faculty from the department with the senior most acting as the Chairperson.

PEC

Societal Project			
Course Code	22SFC35	CIE Marks	100
Number of contact Hours/Week	6	SEE Marks	__
Credits	3	Exam Hours	03

Course objectives:

- Build creative solutions for development problems of current scenario in the Society.
- Utilize the skills developed in the curriculum to solve real life problems.
- Improve understanding and develop methodology for solving complex issues.

Some of the domains to choose for societal projects:

- Infrastructure
- Health Care
- Social security
- Security for women
- Transportation
- Business Continuity
- Remote working and Education
- Digital Finance, Food Security
- Rural employment
- Water and land management
- Pollution, Financial Independence
- Agricultural Finance
- Primary Health care
- Nutrition .Child Care
- E-learning, Distance parenting
- Mentorship Etc

Course outcomes:

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

- Building solution for real life societal problems.
- Improvement of their technical/curriculum skills

Continuous Internal Evaluation:

Identifying the real life problems and producing literature report : 20 marks

Data sampling and Cleaning :10 Marks

Establishing the right Objective: 10 Marks

Developing the solution : 20 Marks

Propagating the solution to the stake holders 1)Lectures 2)Social Meetings 3)Social media 4)Street plays 5)Advertisement Either of the 3(evidence of the work through geo tag photo) Certified by stake holders and authorized by concerned government authorities

Project Report: 20 marks. The basis for awarding the marks shall be the involvement of the student in the project and in the preparation of project report. To be awarded by the internal guide in consultation with external guide if any.

Project Presentation: 10 marks.

The Project Presentation marks of the Project Work Phase -II shall be awarded by the committee constituted for the purpose by the Head of the Department. The committee shall consist of three faculty from the department with the senior most acting as the Chairperson.

Evalution: 10 marks.

The student shall be evaluated based on the ability in the Question and Answer session for 10 marks.

PEC

INTERNSHIP			
Course Code	22SFC36	CIE Marks	50
Number of contact Hours/Week	3	SEE Marks	50
Credits	06	Exam Hours	03

Course objectives:

Internship/Professional practice provide students the opportunity of hands-on experience that include personal training, time and stress management, interactive skills, presentations, budgeting, marketing, liability and risk management, paperwork, equipment ordering, maintenance, responding to emergencies etc. The objective are further,

To put theory into practice.

To expand thinking and broaden the knowledge and skills acquired through course work in the field. To relate to, interact with, and learn from current professionals in the field.

To gain a greater understanding of the duties and responsibilities of a professional. To understand and adhere to professional standards in the field.

To gain insight to professional communication including meetings, memos, reading, writing, public speaking, research, client interaction, input of ideas, and confidentiality.

To identify personal strengths and weaknesses.

To develop the initiative and motivation to be a self-starter and work independently.

Internship/Professional practice: Students under the guidance of internal guide/s and external guide shall take part in all the activities regularly to acquire as much knowledge as possible without causing any inconvenience at the place of internship.

Seminar: Each student, is required to

- Present the seminar on the internship orally and/or through power point slides.
- Answer the queries and involve in debate/discussion.
- Submit the report duly certified by the external guide.
- The participants shall take part in discussion to foster friendly and stimulating environment in which the students are motivated to reach high standards and become self-confident.

Course outcomes:

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

- Gain practical experience within industry in which the internship is done.
- Acquire knowledge of the industry in which the internship is done.
- Apply knowledge and skills learned to classroom work.
- Develop a greater understanding about career options while more clearly defining personal career goals.
- Experience the activities and functions of professionals.
- Develop and refine oral and written communication skills.
- Identify areas for future knowledge and skill development.
- Expand intellectual capacity, credibility, judgment, intuition.
- Acquire the knowledge of administration, marketing, finance and economics.

Continuous Internal Evaluation

CIE marks for the Internship/Professional practice report (30 marks), seminar (10 marks) and question and answer session (10 marks) shall be awarded (based on the quality of report and presentation skill, participation in the question and answer session by the student) by the committee constituted for the purpose by the Head of the Department. The committee shall consist of three faculty from the department with the senior most acting as the Chairperson.

PEC

Semester End Examination
SEE marks for the internship report (20 marks), seminar (20 marks) and question and answer session (10 marks) shall be awarded (based on the quality of report and presentation skill, participation in the question and answer session) by the examiners appointed by the University.

PEC

PROJECT WORK PHASE -2			
Course Code	22SFC41	CIE Marks	100
Practical /Field work/Week	8	SEE Marks	100
Credits	18	Exam Hours	03

Course objectives:

- To support independent learning.
- To guide to select and utilize adequate information from varied resources maintaining 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.

Project Work Phase - II: 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.

- Follow the Software Development life cycle
- Data Collection ,Planning
- Design the Test cases
- Validation and verification of attained results
- Significance of parameters w.r.t scientific quantified data.
- Publish the project work in reputed Journal.

Course outcomes:

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

- Present the project and be able to defend it.
- Make links across different areas of knowledge and to generate, develop and evaluate ideas andinformation 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 oralforms.
- Work in a team to achieve common goal.
- Learn on their own, reflect on their learning and take appropriate actions to improve it.

PEC

Continuous Internal Evaluation:

Project Report: 20 marks. The basis for awarding the marks shall be the involvement of the student in the project and in the preparation of project report. To be awarded by the internal guide in consultation with external guide if any.

Project Presentation: 20 marks.

The Project Presentation marks of the Project Work Phase -II shall be awarded by the committee constituted for the purpose by the Head of the Department. The committee shall consist of three faculty from the department with the senior most acting as the Chairperson.

Project Execution: 50 Marks

The Project Execution marks of the Project Work Phase -II shall be awarded by the committee constituted for the purpose by the Head of the Department. The committee shall consist of three faculty from the department with the senior most acting as the Chairperson.

Question and Answer: 10 marks.

The student shall be evaluated based on the ability in the Question and Answer session for 10 marks.

Semester End Examination

SEE marks for the project report (60 marks), seminar (30 marks) and question and answer session (10 marks) shall be awarded (based on the quality of report and presentation skill, participation in the question and answer session) by the examiners appointed by the University.