VISVESVARAYA TECHNOLOGICAL UNIVERSITY
BELAGAVI

Scheme of Teaching and Examinations and Syllabus

M.Tech in Cyber Security (SCR)

(Effective from Academic year 2020 - 21)

VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI
Scheme of Teaching and Examinations – 2020 - 21

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

I SEMESTER

SL. No.	Course	Course Code	Course Title	Teaching Hours / Week			Examination				Credits
				Theory	Practical / Seminar	Skill Development Activity	Duration in Hours	CIE Marks	SEE Marks	Total Marks	
1	PCC	20SCR11	Mathematical Foundations of Computer Science	03	--	02	03	40	60	100	4
2	PCC	20SCR12	Information and Network Security	03	--	02	03	40	60	100	4
3	PCC	20SCR13	Ethical Hacking	03	--	02	03	40	60	100	4
4	PCC	20SCR14	Cloud Security	03	--	02	03	40	60	100	4
5	PCC	20SCR15	Cyber Security and Cyber law	03	--	02	03	40	60	100	4
6	PCC	20SCRL16	Ethical Hacking Laboratory	--	04	--	03	40	60	100	2
7	PCC	20RMI17	Research Methodology and IPR	01	--	02	03	40	60	100	2
			TOTAL	**16**	**04**	**12**	**21**	**280**	**420**	**700**	**24**

Note: PCC: Profession Core

Skill development activities:

Students and course instructor/s to involve either individually or in groups to interact together to enhance the learning and application skills. The students should interact with industry (small, medium and large), understand their problems or foresee what can be undertaken for study in the form of research/ testing / projects, and for creative and innovative methods to solve the identified problem. The students shall

1. Gain confidence in modelling of systems and algorithms.
2. Work on different software/s (tools) to Simulate, analyze and authenticate the output to interpret and conclude. Operate the simulated system under changed parameter conditions to study the system with respect to thermal study, transient and steady state operations, etc.
3. Handle advanced instruments to enhance technical talent.
4. Involve in case studies and field visits/ field work.
5. Accustom with the use of standards/codes etc., to narrow the gap between academia and industry.

All activities should enhance student's abilities to employment and/or self-employment opportunities, management skills, Statistical analysis, fiscal expertise, etc.

Internship: All the students have to undergo mandatory internship of 6 weeks during the vacation of I and II semesters and /or II and III semesters. A University examination shall be conducted during III semester and the prescribed credit shall be counted for the same semester. Internship shall be considered as a head of passing and shall be considered for the award of degree. Those, who do not take-up/complete the internship shall be declared as fail in internship course and have to complete the same during the subsequent University examination after satisfying the internship requirements.

Note: (i) Four credit courses are designed for 50 hours Teaching – Learning process.
(ii) Three credit courses are designed for 40 hours Teaching – Learning process.

VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI
Scheme of Teaching and Examinations – 2020 - 21

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

II SEMESTER

SL. No.	Course	Course Code	Course Title	Teaching Hours / Week			Examination				Credits
				Theory	**Practical / Seminar**	**Skill Development Activity**	**Duration in Hours**	**CIE Marks**	**SEE Marks**	**Total Marks**	
1	PCC	20SCR21	Network Programming	03	--	02	03	40	60	100	4
2	PCC	20SCR22	Information Security Policies in Industry	03	--	02	03	40	60	100	4
3	PCC	20SCR23	Social Network Analysis	03	--	02	03	40	60	100	4
4	PEC	20SCR24X	Professional elective 1	04	--	--	03	40	60	100	4
5	PEC	20SCR25X	Professional elective 2	04	--	--	03	40	60	100	4
6	PCC	20SCRL26	Network Security & Network Programming Laboratory	--	04	--	03	40	60	100	2
7	PCC	20SCR27	Technical Seminar	--	02	--	--	100	--	100	2
			TOTAL	**17**	**06**	**06**	**18**	**340**	**360**	**700**	**24**

Note: PCC: Profession Core, PEC: Professional Elective Course

Professional Elective-1		Professional Elective-2	
Course Code 20LSCS24X	**Course Title**	**Course Code 20SCS25X**	**Course Title**
20SCR241	Mobile Application Development	20SCR251	Business Intelligence and its Applications
20SCR242	Security Architecture Design	20SCR252	Database Security
20SCR243	Security Assessment and Verification	20SCR253	Software Metrics & Quality Assurance
20SCR244	Blockchain Technology	20SCR254	Advanced Cryptography

Note:

1. Technical Seminar: CIE marks shall be awarded by a committee comprising of HoD as Chairman, Guide/co-guide, if any, and a senior faculty of the department. Participation in the seminar by all postgraduate students of the program shall be mandatory.

The CIE marks awarded for Technical Seminar, shall be based on the evaluation of Seminar Report, Presentation skill and performance in Question and Answer session in the ratio 50:25:25.

2. Internship: All the students shall have to undergo mandatory internship of 6 weeks during the vacation of I and II semesters and /or II and III semesters. A University examination shall be conducted during III semester and the prescribed internship credit shall be counted in the same semester. Internship shall be considered as a head of passing and shall be considered for the award of degree. Those, who do not take-up/complete the internship shall be declared as fail in internship course and have to complete the same during the subsequent University examination after satisfying the internship requirements.

VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI
Scheme of Teaching and Examinations – 2020 - 21

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

III SEMESTER

SL. No.	Course	Course Code	Course Title	Teaching Hours / Week			Examination				Credits
				Theory	Practical / Seminar	Skill Development Activity	Duration in Hours	CIE Marks	SEE Marks	Total Marks	
1	PCC	20SCR31	Machine Learning Techniques	03	--	02	03	40	60	100	4
2	PEC	20SCR32X	Professional elective 3	03	--	--	03	40	60	100	3
3	PEC	20SCR33X	Professional elective 4	03	--	--	03	40	60	100	3
4	Project	20SCR34	Project Work phase -1	--	02	--	--	100	--	100	2
5	PCC	20SCR35	Mini-Project	--	02	--	--	100	--	100	2
6	Internship	20SCRI36	Internship	(Completed during the intervening vacation of I and II semesters and /or II and III semesters.)			03	40	60	100	6
			TOTAL	**09**	**04**	**02**	**12**	**360**	**240**	**600**	**20**

Note: PCC: Profession Core, PEC: Professional Elective Course

Professional Elective-3		Professional Elective-4	
Course Code 20SCS32X	**Course Title**	**Course Code 20SCS33X**	**Course Title**
20SCR321	Operating System Security	20SCR331	Managing Big Data
20SCR322	Data Mining & Data Warehousing	20SCR332	Analysis of Computer Networks
20SCR323	Speech Processing	20SCR333	Natural Language Processing
20SCR324	Trends in Artificial Intelligence and Soft Computing	20SCR334	Deep Learning

Note:

1. Project Work Phase-1: Students in consultation with the guide/co-guide if any, shall pursue literature survey and complete the preliminary requirements of selected Project work. Each student shall prepare relevant introductory project document and present a seminar.

CIE marks shall be awarded by a committee comprising of HoD as Chairman, Guide/co-guide if any, and a senior faculty of the department. The CIE marks awarded for project work phase -1, shall be based on the evaluation of Project Report, Project Presentation skill and Question and Answer session in the ratio 50:25:25. SEE (University examination) shall be as per the University norms.

2. Internship: Those, who have not pursued /completed the internship shall be declared as fail in internship course and have to complete the same during subsequent University examinations after satisfying the internship requirements. Internship SEE (University examination) shall be as per the University norms.

VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI

Scheme of Teaching and Examinations – 2020 - 21

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

IV SEMESTER

Sl. No	Course	Course Code	Course Title	Teaching Hours /Week		Examination				Credits
				Theory	Practical /Field work	Duration in hours	CIE Marks	SEE Marks Viva voce	Total Marks	
				L	P					
1	Project	20SCR41	Project work phase -2	--	04	03	40	60	100	20
			TOTAL	--	**04**	**03**	**40**	**60**	**100**	**20**

Note:

1. Project Work Phase-2:

CIE marks shall be awarded by a committee comprising of HoD as Chairman, Guide/co-guide, if any, and a Senior faculty of the department. The CIE marks awarded for project work phase -2, shall be based on the evaluation of Project Report subjected to plagiarism check, Project Presentation skill and performance in Question and Answer session in the ratio 50:25:25.

SEE shall be at the end of IV semester. Project work evaluation and Viva-Voce examination (SEE), after satisfying the plagiarism check, shall be as per the University norms.

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -I

MATHEMATICAL FOUNDATION OF COMPUTER SCIENCE

Course Code	**20SCR11,** 20LNI11, 20SCS11, 20SCE11, 20SFC11, 20SCN11, 20SSE11, 20SIT11, 20SAM11, 20SIS11	CIE Marks	40
Teaching Hours/Week (L:P:S)	3:0:2	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Vector Spaces: Vector spaces; subspaces Linearly independent and dependent vectors Basis and dimension; coordinate vectors-Illustrative examples. Linear transformations, Representation of transformations by matrices;

(RBT Levels: **L1 & L2)** (Textbook:1)

Module-2

Orthogonality and least squares: Inner product, orthogonal sets, orthogonal projections, orthogonal bases. Gram-Schmidt orthogonalization process. QR factorizations of a matrices, least square problems, applications to linear models (least square lines and least square fitting of other curves).

(RBT Levels: **L2 & L3)** (Textbook:1)

Module-3

Symmetric and Quadratic Forms: Diagonalization, Quadratic forms, Constrained Optimization, The Singular value decomposition. Applications to image processing and statistics, Principal Component Analysis

(RBT Levels: **L2 & L3)** (Textbook:1)

Module-4

Statistical Inference: Introduction to multivariate statistical models: Correlation and Regression analysis, Curve fitting (Linear and Non-linear)

(RBT Levels: **L2 & L3)** (Textbook:3)

Module-5

ProbabilityTheory: Random variable (discrete and continuous), Probability mass function (pmf), Probability density function (pdf), Mathematical expectation, Sampling theory: testing of hypothesis by ***t***-test, χ^2- test.

(RBT Levels: **L1 & L2)** (Textbook:3)

Course Outcomes:

On completion of this course, students are able to:

1. Understand the numerical methods to solve and find the roots of the equations.
2. Apply the technique of singular value decomposition for data compression, least square approximation in solving inconsistent linear systems
3. Understand vector spaces and related topics arising in magnification and rotation of images.
4. Utilize the statistical tools in multi variable distributions.
5. Use probability formulations for new predictions with discrete and continuous RV's.

Question Paper Pattern:

- The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.
- The question paper will have ten full questions carrying equal marks.
- Each full question consisting of 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have 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.

Textbooks:

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Linear Algebra and its Applications	David C. Lay, Steven R. Lay and J. J. McDonald	Pearson Education Ltd	5th Edition 2015.
2	Numerical methods for Scientific and Engg. Computation	M K Jain, S.R.K Iyengar, R K. Jain	New Age International	6th Ed., 2014
3	Probability, Statistics and Random Process	T. Veerarajan	Tata Mc-Graw Hill Co	3rd Edition 2016

Reference books:

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Optimization: Theory & Applications Techniques	Rao. S.S	Wiley Eastern Ltd New Delhi.	
2	Signals, Systems, and Inference	Alan V. Oppenheim and George C. Verghese	Spring	2010.
3	Foundation Mathematics for Computer Science	John Vince	Springer International	
4	Higher Engineering Mathematics	B.S. Grewal	Khanna Publishers	44th Ed.,2017

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -I

INFORMATION AND NETWORK SECURITY

Course Code	**20SCR12,** 20SCN13, 20LNI13 , 20SIS333	CIE Marks	40
Teaching Hours/Week (L:P:S)	3:0:2	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Classical Encryption Techniques Symmetric Cipher Model, Cryptography, Cryptanalysis and Brute-Force 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

Module 2

Public-Key Cryptography and RSA: Principles of public-key cryptosystems. Public-key cryptosystems. Applications for public-key cryptosystems, requirements for public-key cryptosystems. Public-key cryptanalysis. The RSA algorithm, description of the algorithm, computational aspects, the security of RSA. **Other Public-Key Cryptosystems:** Diffie-Hellman key exchange, The algorithm, key exchange protocols, man in the middle attack, Elgamal Cryptographic systems, Elliptic curve arithmetic, abelian groups, elliptic curves over real numbers, elliptic curves over Zp, elliptic curves overGF(2m), Elliptic curve cryptography, Analog of Diffie-Hellman key exchange, Elliptic curve encryption/ decryption, security of Elliptic curve cryptography, Pseudorandom number generation based on an asymmetric cipher, PRNG based on RSA.

Module 3

Key Management and Distribution: Symmetric key distribution using Symmetric encryption, A key distribution scenario, Hierarchical key control, session key lifetime, a transparent key control scheme, Decentralized key control, controlling key usage, Symmetric key distribution using asymmetric encryption, simple secret key distribution, secret key distribution with confidentiality and authentication, A hybrid scheme, distribution of public keys, public announcement of public keys, publicly available directory, public key authority, public keys certificates, X-509 certificates. Certificates, X-509 version 3, public key infrastructure. **User Authentication:** Remote user Authentication principles, Mutual Authentication, one way Authentication, remote user Authentication using Symmetric encryption, Mutual Authentication, one way Authentication, Kerberos, Motivation , Kerberos version 4, Kerberos version 5, Remote user Authentication using Asymmetric encryption, Mutual Authentication, one way Authentication, federated identity management, identity management, identity federation, personal identity verification.

Module 4

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, protected data transfer phase, the IEEE 802.11i pseudorandom function. W**eb 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, Cryptographic Computations, and Padding. **HTTPS** Connection Initiation, Connection Closure. **Secure Shell(SSH)** Transport Layer Protocol, User Authentication Protocol, Connection Protocol

Module 5

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.

Course outcomes:

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

- Analyze the vulnerabilities in any computing system and hence be able to design a security solution.
- Identify the security issues in the network and resolve it.
- Evaluate security mechanisms using rigorous approaches, including theoretical.

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- 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 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.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Cryptography and Network Security	William Stallings	Pearson	6th edition

Reference Books

1	Cryptography and Information Security	V K Pachghare	PHI	2nd

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -I

ETHICAL HACKING

Course Code	**20SCR13,**20SFC12	CIE Marks	40
Teaching Hours/Week (L:P:S)	3:0:2	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

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

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.

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.

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.

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.

Course outcomes:

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

- Explain aspects of security, importance of data gathering, foot printing and system hacking.
- Explain aspects of security, importance of data gathering, foot printing and system hacking.
- Demonstrate how intruders escalate privileges.
- Demonstrate how intruders escalate privileges.
- Demonstrate how intruders escalate privileges.

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- 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 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.

Textbook/ Textbooks				
Sl No	**Title of the book**	**Name of the Author/s**	**Publisher Name**	**Edition and year**
1	Hacking Exposed 7: Network Security Secrets & Solutions	Stuart McClure, Joel Scambray and Goerge Kurtz	Tata McGraw Hill Publishers	2010
2	Microsoft Windows Security Resource Kit	Bensmith, and Brian Komer	Prentice Hall of India	2010
Reference Books				
1	Hacking Exposed Network Security Secrets & Solutions	Stuart McClure, Joel Scambray and Goerge Kurtz	Tata McGraw Hill Publishers	5th Edition2010
3	Gray Hat Hacking The Ethical Hackers Handbook	Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle	McGraw-Hill Osborne Media paperback	3rd Edition,2011

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -I

CLOUD SECURITY

Course Code	**20SCR14,** 20SFC15, 20LNI333, 20SCE331	CIE Marks	40
Teaching Hours/Week (L:P:S)	3:0:2	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

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.

Module 2

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.

Module 3

Traditional Security, Business Continuity, Disaster Recovery, Risk of insider abuse, Security baseline, Customers actions, Contract, Documentation, Recovery Time Objectives (RTOs), Customers responsibility, Vendor Security Process (VSP).

Module 4

Data Center Operations: Data Center Operations, Security challenge, Implement Five Principal Characteristics of Cloud Computing, Data center Security Recommendations. Encryption and Key Management: Encryption for Confidentiality and Integrity, Encrypting data at rest, Key Management Lifecycle, Cloud Encryption Standards, Recommendations.

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.

Course outcomes:

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

- Demonstrate the growth of Cloud computing, architecture and different modules of implementation.

- Evaluate the different types of cloud solutions among IaaS, PaaS, SaaS.
- Access the security implementation flow, actions and responsibilities of stake holders.
- Generalize the Data Centre operations, encryption methods and deployment details.
- Provide recommendations for using and managing the customer's identity and choose the type of virtualization to be used.

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- 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 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.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Cloud Security and Privacy, An Enterprise Perspective on Risks and Compliance	Tim Mather, Subra Kumaraswamy, Shahed Latif	Oreilly Media	2009

Reference Books

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Securing the Cloud, Cloud Computer Security Techniques and Tactics	Vic (J.R.) Winkler	Syngress	2011

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -I

CYBER SECURITY AND CYBER LAW

Course Code	**20SCR15,** 20LNI244, 20SCE244, 20SIT244, 20SAM244	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Introduction to Cybercrime: Cybercrime: Definition and Origins of the Word, Cybercrime and Information Security, Who are Cybercriminals?, Classifications of Cybercrimes, Cybercrime: The Legal Perspectives, Cybercrimes: An Indian Perspective, Cybercrime and the Indian ITA 2000, A Global Perspective on Cybercrimes, Cybercrime Era: Survival Mantra for the Netizens. Cyberoffenses: How Criminals Plan Them: How Criminals Plan the Attacks, Social Engineering, Cyberstalking, Cybercafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Attack Vector, Cloud Computing.

Module -2

Cybercrime: Mobile and Wireless Devices: Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication Service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for organizations, Organizational Measures for Handling Mobile, Organizational Security Policies and Measures in Mobile Computing Era, Laptops

Module – 3

Tools and Methods Used in Cybercrime: Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Keyloggers and Spywares, Virus and Worms, Trojan Horses and Backdoors, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks. Phishing and Identity Theft: Introduction, Phishing, Identity Theft (ID Theft).

Module-4

Understanding Computer Forensics: Introduction, Historical Background of Cyberforensics, Digital Forensics Science, The Need for Computer Forensics, Cyberforensics and Digital Evidence, Forensics Analysis of E-Mail, Digital Forensics Life Cycle, Chain of Custody Concept, Network Forensics, Approaching a Computer Forensics Investigation, Setting up a Computer Forensics Laboratory: Understanding the Requirements, Computer Forensics and Steganography, Relevance of the OSI 7 Layer Model to Computer Forensics, Forensics and Social Networking Sites: The Security/Privacy Threats, Computer Forensics from Compliance Perspective, Challenges in Computer Forensics, Special Tools and Techniques, Forensics Auditing, Antiforensics.

Module-5

Introduction to Security Policies and Cyber Laws: Need for An Information Security Policy, Information Security Standards – Iso, Introducing Various Security Policies and Their Review Process, Introduction to Indian Cyber Law, Objective and Scope of the it Act, 2000, Intellectual Property Issues, Overview of Intellectual - Property - Related Legislation in India, Patent, Copyright, Law Related to Semiconductor Layout and Design, Software License.

Course outcomes:

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

- Define cyber security, cyber law and their roles
- Demonstrate cyber security cybercrime and forensics.
- Infer legal issues in cybercrime,
- Demonstrate tools and methods used in cybercrime and security.
- Illustrate evidence collection and legal challenges

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- 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 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.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives	SunitBelapure and Nina Godbole	Wiley India Pvt Ltd	2013
2	Introduction to information security and cyber laws	Surya Prakash Tripathi, Ritendra Goyal, Praveen Kumar Shukla	Dreamtech Press	2015

Reference Books

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions	Thomas J. Mowbray	John Wiley & Sons,	
2	Cyber Security Essentials	James Graham, Ryan Olson, Rick Howard	CRC Press	2010

M.TECH IN CYBER SECURITY (SCR) Choice Based Credit System (CBCS) and Outcome Based Education (OBE) SEMESTER -I			
ETHICAL HACKING LABORATORY			
Course Code	**20SCRL16**	CIE Marks	40
Teaching Hours/Week (L:P:S)	0:4:0	SEE Marks	60
Credits	02	Exam Hours	03

List of 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. 4.
5. HTTrack: Website mirroring using Httrack and hosting on a local network.
6. XSS: Inject a client side script to a web application.
7. Emailtrackerpro: Email analysis involving header check, tracing the route. Also perform a check on a spam mail and non-spam mail.

Course outcomes:

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

- Evaluate modern tools
- Analyze packet capturing in network
- Define forensic analysis
- Security in various web applications

Conduction of Practical Examination:

All laboratory experiments (nos) are to be included for practical examination.

Studentsare allowed to pick one experimentfrom **each part and execute both**

Strictlyfollow theinstructions as printed on the cover page of answerscript for breakup of marks

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

Textbook/ Textbooks

Sl No	**Title of the book**	**Name of the Author/s**	**Publisher Name**	**Edition and year**
1				

Reference Books

1				

RESEARCH METHODOLOGY AND IPR

Course Code	20RMI17	CIE Marks	40
Teaching Hours/Week (L:P:SDA)	1:0:2	SEE Marks	60
Credits	02	Exam Hours	03

Module-1

Research Methodology: Introduction, Meaning of Research, Objectives of Research, Motivation in Research, Types of Research, Research Approaches, Significance of Research, Research Methods versus Methodology, Research and Scientific Method, Importance of Knowing How Research is Done, Research Process, Criteria of Good Research, and Problems Encountered by Researchers in India.

Defining the Research Problem: Research Problem, Selecting the Problem, Necessity of Defining the Problem, Technique Involved in Defining a Problem, An Illustration. ■

Module-2

Reviewing the literature: Place of the literature review in research, Bringing clarity and focus to your research problem, Improving research methodology, Broadening knowledge base in research area, Enabling contextual findings, How to review the literature, searching the existing literature, reviewing the selected literature, Developing a theoretical framework, Developing a conceptual framework, Writing about the literature reviewed. **Research Design:** Meaning of Research Design, Need for Research Design, Features of a Good Design, Important Concepts Relating to Research Design, Different Research Designs, Basic Principles of Experimental Designs, Important Experimental Designs. ■

Module-3

Design of Sampling: Introduction, Sample Design, Sampling and Non-sampling Errors, Sample Survey versus Census Survey, Types of Sampling Designs.

Measurement and Scaling: Qualitative and Quantitative Data, Classifications of Measurement Scales, Goodness of Measurement Scales, Sources of Error in Measurement Tools, Scaling, Scale Classification Bases, Scaling Technics, Multidimensional Scaling, Deciding the Scale.

Data Collection: Experimental and Surveys, Collection of Primary Data, Collection of Secondary Data, Selection of Appropriate Method for Data Collection, Case Study Method. ■

Module-4

Testing of Hypotheses: Hypothesis, Basic Concepts Concerning Testing of Hypotheses, Testing of Hypothesis, Test Statistics and Critical Region, Critical Value and Decision Rule, Procedure for Hypothesis Testing, Hypothesis Testing for Mean, Proportion, Variance, for Difference of Two Mean, for Difference of Two Proportions, for Difference of Two Variances, P-Value approach, Power of Test, Limitations of the Tests of Hypothesis.

Chi-square Test: Test of Difference of more than Two Proportions, Test of Independence of Attributes, Test of Goodness of Fit, Cautions in Using Chi Square Tests. ■

Module-5

Interpretation and Report Writing: Meaning of Interpretation, Technique of Interpretation, Precaution in Interpretation, Significance of Report Writing, Different Steps in Writing Report, Layout of the Research Report, Types of Reports, Oral Presentation, Mechanics of Writing a Research Report, Precautions for Writing Research Reports.

Intellectual Property: The Concept, Intellectual Property System in India, Development of TRIPS Complied Regime in India, Patents Act, 1970, Trade Mark Act, 1999,The Designs Act, 2000, The Geographical Indications of Goods (Registration and Protection) Act1999, Copyright Act,1957,The Protection of Plant Varieties and Farmers' Rights Act, 2001,The Semi-Conductor Integrated Circuits Layout Design Act, 2000, Trade Secrets, Utility Models, IPR and Biodiversity, The Convention on Biological Diversity (CBD) 1992, Competing Rationales for Protection of IPRs, Leading International Instruments Concerning IPR, World Intellectual Property Organisation (WIPO),WIPO and WTO, Paris Convention for the Protection of Industrial Property, National Treatment, Right of Priority, Common Rules, Patents, Marks, Industrial Designs, Trade Names, Indications of Source, Unfair Competition,

Patent Cooperation Treaty (PCT), Advantages of PCT Filing, Berne Convention for the Protection of Literary and Artistic Works, Basic Principles, Duration of Protection, Trade Related Aspects of Intellectual Property Rights(TRIPS) Agreement, Covered under TRIPS Agreement, Features of the Agreement, Protection of Intellectual Property under TRIPS, Copyright and Related Rights, Trademarks, Geographical indications, Industrial Designs, Patents, Patentable Subject Matter, Rights Conferred, Exceptions, Term of protection, Conditions on Patent Applicants, Process Patents, Other Use without Authorization of the Right Holder, Layout- Designs of Integrated Circuits, Protection of Undisclosed Information, Enforcement of Intellectual Property Rights,

UNSECO. ■

Course outcomes:

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

- Discuss research methodology and the technique of defining a research problem
- Explain the functions of the literature review in research, carrying out a literature search, developing theoretical and conceptual frameworks and writing a review.
- Explain various research designs, sampling designs, measurement and scaling techniques and also different methods of data collections.
- Explain several parametric tests of hypotheses, Chi-square test, art of interpretation and writing research reports
- Discuss various forms of the intellectual property, its relevance and business impact in the changing global business environment and leading International Instruments concerning IPR. ■

Question paper pattern:

- The question paper will have ten questions.
- Each full question is for 20 marks.
- There will be 2 full questions (with a maximum of four sub questions in one full question) from each module.
- Each full question with sub questions will cover the contents under a module.
- Students will have to answer 5 full questions, selecting one full question from each module.■

Textbooks

1. Research Methodology: Methods and Techniques, C.R. Kothari, Gaurav Garg, New Age International, 4th Edition, 2018.
2. Research Methodology a step-by-step guide for beginners. Ranjit Kumar, SAGE Publications, 3rd Edition, 2011. (For the topic Reviewing the literature under module 2),
3. Study Material, (For the topic Intellectual Property under module 5), Professional Programme Intellectual
4. Property Rights, Law and Practice, The Institute of Company Secretaries of India, Statutory Body Under an Act of Parliament, September 2013.

Reference Books

1. Research Methods: the concise knowledge base, Trochim, Atomic Dog Publishing, 2005.
2. Conducting Research Literature Reviews: From the Internet to Paper, Fink A, Sage Publications, 2009.

M.Tech. in CYBER SECURITY(SCR) Choice Based Credit System (CBCS) and Outcome Based Education(OBE) **SEMESTER -II**			
NETWORK PROGRAMMING			
Course Code	**20SCR21,** 20LNI14, 20SCN22	CIE Marks	40
TeachingHours/Week (L:P:S)	3:0:2	SEE Marks	60
Credits	04	Exam Hours	03
Module-1			
Introduction to network application, client/server communication, OSI Model, BSD Networking history, Test Networks and Hosts, Unix Standards, 64-bit architectures, Transport Layer: TCP, UDP and SCTP.			
Module 2			
Sockets Introduction – socket address structures, value-result arguments, byte ordering and manipulation functions, address conversion functions, Elementary TCP Sockets – socket, connect, bind, listen, accept , fork and concurrent server design, getcsockname and getpeername functions and TCP Client/Server Example- client/server programming through TCP sockets, Normal startup, termination, POSIX signal handling, Signal handling in server, Crashing, rebooting of server host, shutdown			
Module 3			
I/O Multiplexing and Socket Options, Elementary SCTP Sockets- Interface Models, sctp_xx functions, shutdown function, Notifications, SCTP Client/Server Examples – One-to-Many, Head–of-Line			

Blocking, Controlling number of streams and Termination, IPv4 and IPv6 Interoperability–different interoperability scenarios.

Module 4

Daemon Processes, syslogd, daemonizing functions and the inetd super server, Advanced I/O functions- readv, writev, sendmsg and recvmsg, Ancillary data, Advanced polling, Unix domain protocols- socket address structure, functions and communication scenarios, Nonblocking I/O – connect and accept examples.

Module 5

ioctl operations- socket, file, interface configuration information, ARP cache and routing table operations, Routing sockets- data link socket address structure, reading and writing, sysctl operations, interface name and index functions, Key Management functions – reading, writing, SADB, SA, Dynamically Maintaining SA's, Out-of-Band data, Threads- basic thread functions, TCP echo server using threads, Mutexes and Conditional variables.

Course outcomes:

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

- Develop applications that communicate with each other using TCP and SCTP.
- Identify the IPv4 and IPv6 compatibility.
- Evaluate socket programming APIs.

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- 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 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.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	UNIX Network Programming	W. Richard Stevens, Bill Fenner, Andrew M. Rudoff	Pearson	Volume 1, Third Edition, 2004

Reference Books

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Network Programming in C	Barry Nance	PHI	2002
2	Windows Socket Network Programming	Bob Quinn, Dave Shute	Pearson	2003.
3	UNIX Network Programming	Richard Stevens		Second Edition.

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -II

INFORMATION SECURITY POLICIES IN INDUSTRY

Course Code	**20SCR22,** 20SFC243, 20SCN323	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

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

Law Enforcement, Security awareness training and support.

Module 2

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

Module 3

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

Module 4

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

Module 5

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

Course outcomes:

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

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

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- 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 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.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Writing Information Security Policies	Scott Barman	Sams Publishing	2002
2	Information Policies Procedures and Standards	Thomas.R.Peltier	CRC Press	2004

Reference Books

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Information Security Fundamentals	Thomas R Peltier, Justin Peltier, John Backley	CRC Press,	2005
2	Information Security Management Handbook	Harold F. Tipton and Micki Krause	Auerbach publications	5th Edition, 2005

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -II

SOCIAL NETWORK ANALYSIS

Course Code	**20SCR23,** 20SFC333, 20LNI332, 20SCN252	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Introduction to social network analysis and Descriptive network analysis: Introduction to new science of networks. Networks examples. Graph theory basics. Statistical network properties. Degree distribution, clustering coefficient. Frequent patterns. Network motifs. Cliques and k-cores.

Module 2

Network structure, Node centralities and ranking on network: Nodes and edges, network diameter and average path length. Node centrality metrics: degree, closeness and betweenness centrality. Eigenvector centrality and PageRank. Algorithm HITS.

Module 3

Network communities and Affiliation networks: Networks communities. Graph partitioning and cut metrics. Edge betweenness. Modularity clustering. Affiliation network and bipartite graphs. 1-mode projections. Recommendation systems.

Module 4

Information and influence propagation on networks and Network visualization: Social Diffusion. Basic cascade model. Influence maximization. Most influential nodes in network. Network visualization and graph layouts. Graph sampling. Low -dimensional projections

Module 5

Social media mining and SNA in real world: FB/VK and Twitter analysis: Natural language processing and sentiment mining. Properties of large social networks: friends, connections, likes, re-tweets.

Course outcomes:

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

- Define notation and terminology used in network science.
- Demonstrate, summarize and compare networks.
- Explain basic principles behind network analysis algorithms.
- Analyzing real world network.

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- 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 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.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Networks, Crowds, and Markets: Reasoning About a Highly Connected World	David Easley and John Kleinberg	Cambridge University Press	2010
2	Statistical Analysis of Network Data with R	Eric Kolaczyk, Gabor Csardi	Springer	2014
3	Social Network Analysis. Methods and Applications	Stanley Wasserman and Katherine Faust	Cambridge University Press	1994

Reference Books				

M.Tech. in CYBER SECURITY(SCR) Choice Based Credit System (CBCS) and Outcome Based Education(OBE) SEMESTER -II			
MOBILE APPLICATION DEVELOPMENT			
Course Code	**20SCR241,** 20SFC332, 20LNI323, 20SCN244, 20SIT241, 20SIS252	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Introduction to mobile communication and computing: Introduction to mobile computing, Novel applications, limitations and GSM architecture, Mobile services, System architecture, Radio interface, protocols, Handover and security. Smart phone operating systems and smart phones applications.

Module -2

Fundamentals of Android Development: Introduction to Android., The Android 4.1 Jelly Bean SDK, Understanding the Android Software Stack, Installing the Android SDK, Creating Android Virtual Devices, Creating the First Android Project, Using the Text View Control, Using the Android Emulator.

Module – 3

The Intent of Android Development, Four kinds of Android Components: Activity, Service, Broadcast Receiver and Content Provider. Building Blocks for Android Application Design, Laying Out Controls in Containers. Graphics and Animation: Drawing graphics in Android, Creating Animation with Android's Graphics API.

Module-4

Creating the Activity, Working with views: Exploring common views, using a list view, creating custom views, understanding layout. Using Selection Widgets and Debugging Displaying and Fetching Information Using Dialogs and Fragments. Multimedia: Playing Audio, Playing Video and Capturing Media. Advanced Android Programming: Internet, Entertainment, and Services.

Module-5

Displaying web pages and maps, communicating with SMS and emails. Creating and using content providers: Creating and consuming services, publishing android applications

Course outcomes:

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

- Describe the requirements for mobile applications
- Explain the challenges in mobile application design and development
- Develop design for mobile applications for specific requirements
- Implement the design using Android SDK
- Implement the design using Objective C and iOS
- Deploy mobile applications in Android and iPone marketplace for distribution

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- 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 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.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Mobile Computing: (technologies and Applications	N. N. Jani	S chand	
2	Android programming	B.M.Hirwani	Pearson publications	2013
3	Android in Action	W. Frank Ableson, Robi Sen and C. E. Ortiz	DreamTech Publisher	Third Edition-2012

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -II

SECURITY ARCHITECTURE DESIGN

Course Code	**20SCR242,** 20SFC321	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

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

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.

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.

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.

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.

Course outcomes:

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

- Design the secured sites based on tools & techniques
- Map site zones with level of security
- Identify the components targeted for each zone

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- 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 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.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Designing Security Architecture Solutions	Jay Ramachandran	Wiley Computer Publishing	2010.

Reference Books

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

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -II

SECURITY ASSESSMENT AND VERIFICATION

Course Code	**20SCR243,** 20SFC324	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

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.

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.

Module 3

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

Module 4

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

Module 5

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

Course outcomes:

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

- Illustrate the roles information security and its management
- Select appropriate techniques to tackle and solve problems in the discipline of information security assessment
- Design an information security and validation system

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- 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 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.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	A practical guide to security assessments	Sudhanshu Kairab	CRC press	2005
2	A Security risk assessment Handbook	Douglas J. Landoll	Auerbach publications	2006

Reference Books

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Principles of Information Security	Michael E. Whitman, Herbert J. Mattord	Cengage Learning	2nd Edition
2	Information Security Fundamentals	Thomas R Peltier, Justin Peltier and John Blackley	Prentice Hall	2nd Edition, 1996

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -II

BLOCKCHAIN TECHNOLOGY

Course Code	**20SCR244,** 20SCS23, 20SCN15	CIE Marks	40
TeachingHours/Week (L:T:P)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Blockchain 101; The growth of blockchain technology, Distributed systems, The history of blockchain and Bitcoin, Electronic cash, Blockchain, Blockchain defined, Generic elements of a blockchain, Benefits and limitations of blockchain, Tiers of blockchain technology, Features of a blockchain, Types of blockchain, Consensus, CAP theorem and blockchain.

Decentralization; Decentralization using blockchain, Methods of decentralization, Routes to decentralization, Blockchain and full ecosystem decentralization, Smart contracts, Decentralized Organizations, Platforms for decentralization.

Module-2

Symmetric Cryptography,Working with the OpenSSL command line, Introduction, Mathematics, Cryptographic primitives, Symmetric cryptography, Stream ciphers, Block ciphers, Data Encryption Standard, Advanced Encryption Standard, How AES works.

Public Key Cryptography, Asymmetric cryptography, Public and private keys, RSA, Encryption and decryption using RSA, Elliptic Curve Cryptography, Mathematics behind ECC, Point addition, Point doubling, Discrete logarithm problem in ECC, RSA using OpenSSL, RSA public and private key pair, Private key, Public key, Exploring the public key, Encryption and decryption, Encryption, Decryption, ECC using OpenSSL, ECC private and public key pair, Private key, Private key generation, Hash functions, Secure Hash Algorithms, Merkle trees, Patricia trees, Distributed Hash Tables, Digital signatures, RSA digital signature algorithm, Sign then encrypt, Encrypt then sign. Elliptic Curve Digital Signature Algorithm, How to generate a digital signature using OpenSSL, ECDSA using OpenSSL, Homomorphic encryption, Signcryption, Zero-Knowledge Proofs. Blind signatures, Encoding schemes, Financial markets and trading, Trading, Exchanges, Trade life cycle, Order anticipators, Market manipulation, ,

Module-3

Introducing Bitcoin, Bitcoin, Bitcoin definition, Bitcoin; a bird's-eye view, Sending a payment to someone, Digital keys and addresses, Private keys in Bitcoin, Public keys in Bitcoin, Addresses in Bitcoin, Base58Check encoding, Vanity addresses, Multisignature addresses, Transactions, The transaction life cycle, Transaction fee, Transaction pools, The transaction data structure, Metadata, Inputs, Outputs, Verification, The script language, Commonly used opcodes, Types of transactions, Coinbase transactions, Contracts, Transaction veri&#xFB01;cation, Transaction malleability, Blockchain, The structure of a block, The structure of a block header, The genesis block, Mining. **Bitcoin Network and Payments,** The Bitcoin network, Wallets. Bitcoin payments, Innovation in Bitcoin, **Bitcoin Clients and APIs**, Bitcoin installation, Types of Bitcoin Core clients, Bitcoind, Bitcoin-cli, Bitcoin-qt, Setting up a Bitcoin node, Setting up the source code, Setting up bitcoin.conf, Starting up a node in testnet, Starting up a node in regtest, Experimenting with Bitcoin-cli, Bitcoin programming and the command-line interface.

Module-4

Alternative Coins, Theoretical foundations, Alternatives to Proof of Work, Proof of Storage, Proof of Stake (PoS), Various stake types, Proof of coinage, Proof of Deposit (PoD), Proof of Burn, Proof of Activity (PoA), Nonoutsourceable puzzles, Difficulty adjustment and retargeting algorithms, Kimoto Gravity Well, Dark Gravity Wave, DigiShield, MIDAS, Bitcoin limitations, Privacy and anonymity, Mixing protocols, Third-party mixing protocols, Inherent anonymity, Extended protocols on top of Bitcoin, Colored coins, Counterparty, Development of altcoins, Consensus algorithms, Hashing algorithms, Difficulty adjustment algorithms, Inter-block time, Block rewards, Reward halving rate, Block size and transaction size, Interest rate, Coinage, Total supply of coins, Namecoin, Trading Namecoins, Obtaining Namecoins, Generating Namecoin records, Litecoin, Primecoin, Trading Primecoin, Mining guide, Zcash, Trading Zcash, Mining guide, Address generation, GPU mining, Downloading and compiling nheqminer, Initial Coin Offerings (ICOs), ERC20 tokens, Summary, **Smart Contracts,** History, Definition, Ricardian contracts, Smart contract templates, Oracles, Smart Oracles, Deploying smart contracts on a blockchain, The DAO.

Module-5

Ethereum 101, Introduction, The yellow paper, Useful mathematical symbols, Ethereum blockchain, Ethereum &#x2013; bird's eye view, The Ethereum network, Mainnet, Testnet, Private net, Components of the Ethereum ecosystem, Keys and addresses, Accounts, Types of accounts, Transactions and messages, Contract creation transaction, Message call transaction, Messages, Calls, Transaction validation and execution, The transaction substate, State storage in the Ethereum blockchain, The world state, The account state, Transaction receipts, Ether cryptocurrency / tokens (ETC and ETH), The Ethereum Virtual Machine (EVM), Execution environment, Machine state, The iterator function, Smart contracts, Native contracts.

Course outcomes:

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

- Define and Explain the fundamentals of Blockchain
- Illustrate the technologies of blockchain
- Decribe the models of blockchain
- Analyze and demonstrate the Ethereum
- Analyze and demonstrate Hyperledger fabric

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- 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 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.

Textbook/ Textbooks				
Sl No	**Title of the book**	**Name of the Author/s**	**Publisher Name**	**Edition and year**
1	Mastering Blockchain	Imran Bashir	O'Reilly 9781788839044	2nd Edition, 2018
Reference Books				
1	Mastering Blockchain	Lorne Lantz, Daniel Cawrey	O'Reilly	2020

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -II

BUSINESS INTELLIGENCE AND ITS APPLICATIONS

Course Code	**20SCR251,** 20SCS331, 20SIT252	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Development Steps, BI Definitions, BI Decision Support Initiatives, Development Approaches, Parallel Development Tracks, BI Project Team Structure, Business Justification, Business Divers, Business Analysis Issues, Cost – Benefit Analysis, Risk Assessment, Business Case Assessment Activities, Roles Involved In These Activities, Risks Of Not Performing Step, Hardware, Middleware, DBMS Platform, Non Technical Infrastructure Evaluation

Module -2

Managing The BI Project, Defining And Planning The BI Project, Project Planning Activities, Roles And Risks Involved In These Activities, General Business Requirement, Project Specific Requirements, Interviewing Process

Module – 3

Differences in Database Design Philosophies, Logical Database Design, Physical Database Design, Activities, Roles And Risks Involved In These Activities, Incremental Rollout, Security Management, Database Backup And Recovery

Module-4

Growth Management, Application Release Concept, Post Implementation Reviews, Release Evaluation Activities, The Information Asset and Data Valuation, Actionable Knowledge – ROI, BI Applications, The Intelligence Dashboard

Module-5

Business View of Information technology Applications: Business Enterprise excellence, Key purpose of using IT, Type of digital data, basics f enterprise reporting, BI road ahead.

Course outcomes:

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

- Explain the complete life cycle of BI/Analytical development
- Illustrate technology and processes associated with Business Intelligence framework
- Demonstrate a business scenario, identify the metrics, indicators and make recommendations to achieve the business goal.

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- 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 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.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Business Intelligence Roadmap: The Complete Project Lifecycle for Decision Support Applications	Larissa T Moss and ShakuAtre	Addison Wesley Information Technology Series	2003.
2	Fundamentals of Business Analytics	R N Prasad, SeemaAcharya	Wiley India	2011.
Reference Books				
1	Business Intelligence: The Savvy Manager's Guide	David Loshin	Morgan Kaufmann	
2	Delivering Business Intelligence with Microsoft SQL Server 2005	Brian Larson	McGraw Hill	2006
3	Foundations of SQL Server 2008 Business Intelligence	Lynn Langit	Apress	2011

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -II

DATABASE SECURITY

Course Code	**20SCR252,** 20SFC252, 20SSE333, 20SCE332, 20SIT332	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Introduction: Introduction to Databases, Security Problems in Databases Security Controls Conclusions. Security Models 1: Introduction, Access Matrix Model, Take-Grant Model, Acten Model, PN Model, Hartson and Hsiao's Model, Fernandez's Model, Bussolati and Martella's Model for Distributed databases.

Module 2

Security Models 2: Bell and LaPadula's Model, Biba's Model, Dion's Model, Sea View Model, Jajodia and Sandhu's Model, The Lattice Model for the Flow Control conclusion. Security Mechanisms: Introduction, User Identification/Authentication, Memory Protection, Resource Protection, Control Flow Mechanisms, Isolation, Security Functionalities in Some Operating Systems, Trusted Computer System, Evaluation Criteria.

Module 3

Security Software Design: Introduction, A Methodological Approach to Security, Software Design, Secure Operating System Design, Secure DBMS Design, Security Packages, Database Security Design.

Module 4

Statistical Database Protection & Intrusion Detection Systems: Introduction, Statistics, Concepts and Definitions, Types of Attacks, Inference Controls, evaluation Criteria for Control Comparison, Introduction IDES System, RETISS System, ASES System Discovery.

Module 5

Models For The Protection Of New Generation Database Systems 1: Introduction, A Model for the Protection of Frame Based Systems, A Model for the Protection of Object-Oriented Systems, SORION Model for the Protection of Object-Oriented Databases. Models For The Protection Of New Generation Database Systems 2: A Model for the Protection of New Generation Database Systems, the Orion Model, Jajodia and Kogan's Model, A Model for the Protection of Active Databases Conclusions.

Course outcomes:

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

- Carry out a risk analysis for a large database
- Implement identification and authentication procedures, fine-grained access control and data encryption techniques
- Set up accounts with privileges and roles

- Audit accounts and the database system

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- 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 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.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Database Security and Auditing	Hassan A. Afyoun	CENGAGE Learning	2009
2	Database Security	Castano	Pearson Education	
Reference Books				
1	Database security	Alfred Basta, Melissa Zgola	CENGAGE learning	

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -II

SOFTWARE METRICS & QUALITY ASSURANCE

Course Code	**20SCR253,** 20SFC334, 20SIT243, 20SSE242	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

What Is Software Quality: Quality: Popular Views, Quality Professional Views, Software Quality, Total Quality Management and Summary. **Fundamentals Of Measurement Theory:** Definition, Operational Definition, And Measurement, Level Of Measurement, Some Basic Measures, Reliability And Validity, Measurement Errors, Be Careful With Correlation, Criteria For Causality, Summary. **Software Quality Metrics Overview:** Product Quality Metrics, In Process Quality Metrics, Metrics for Software Maintenance, Examples For Metrics Programs, Collecting Software Engineering Data.

Module -2

Applying The Seven Basic Quality Tools In Software Development: Ishikawa's Seven Basic Tools, Checklist, Pareo Diagram, Histogram, Run Charts, Scatter Diagram, Control Chart, Cause And Effect Diagram. **The Rayleigh Model:** Reliability Models, The Rayleigh Model Basic Assumptions, Implementation, Reliability And Predictive Validity.

Module – 3

Complexity Metrics And Models: Lines Of Code, Halstead's Software Science , Cyclomatic Complexity Syntactic Metrics, An Example Of Module Design Metrics In Practice .**Metric And Lessons Learned For Object Oriented Projects:** Object Oriented Concepts And Constructs, Design And Complexity Metrics, Productivity Metrics, Quality And Quality Management Metrics, Lessons Learned For object oriented Projects.

Module-4

Availability Metrics: Definition And Measurement Of System Availability, Reliability Availability And Defect Rate, Collecting Customer Outage Data For Quality Improvement, In Process Metrics For Outage And Availability .**Conducting Software Project Assessment :**Audit Ad Assessment , Software Process Maturity Assessment And Software Project Assessment , Software Process Assessment A Preponed Software Project Assessment Method.

Module-5

Dos And Don'ts Of Software Process Improvement : Measuring Process Maturity, Measuring Process Capability, Staged Versus Continuous Debating Religion, Measuring Levels Is Not Enough, Establishing The Alignment Principle , Take Time Getting Faster, Keep it Simple Or Face

Decomplexification, Measuring The Value Of Process Improvement , Measuring Process Compliance , Celebrate The Journey Not Just The Destination. **Using Function Point Metrics to Measure Software Process Improvement: Software** Process Improvement Sequences, Process Improvement Economies, Measuring Process Improvement at Activity Levels

Course outcomes:

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

- Identify and apply various software metrics, which determines the quality level of software
- Identify and evaluate the quality level of internal and external attributes of the software product
- Compare and Pick out the right reliability model for evaluating the software
- Evaluate the reliability of any given software product
- Design new metrics and reliability models for evaluating the quality level of the software based on the requirement

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- 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 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.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Metrics and Models in Software Quality Engineering,	Stephen H Khan	Pearson	2nd edition 2013

Reference Books

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Software Metrics	Norman E-Fentor and Share Lawrence Pflieger	International Thomson Computer Press	1997
2	Software quality and Testing Market,.	S.A.Kelkar	PHI Learning, Pvt, Ltd	2012
3	Managing the Software Inc,.	Watts S Humphrey	Process Pearson Education	2008
4	CMMI	Mary Beth Chrissis, Mike Konrad and Sandy	Pearson Education(Singapore	2003
5	Quality is Free: The Art of Making Quality Certain	Philip B Crosby	Mass Market	1992

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -II

ADVANCED CRYPTOGRAPHY

Course Code	**20SCR254,** 20SCS241, 20LNI254	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Number Theory: Introduction to number theory, Overview of modular arithmetic, discrete logarithms, and primality/factoring, Euclid's algorithm, Finite fields, Prime numbers, Fermat's and Euler's theorem-Testing for primality.

Module-2

Symmetric & Asymmetric Cryptography: Classical encryption techniques, Block cipher design principles and modes of operation, Data encryption standard, Evaluation criteria for AES, AES cipher, Principles of public key cryptosystems, The RSA algorithm, Key management – Diffie Hellman Key exchange, Elliptic curve arithmetic-Elliptic curve cryptography.

Module-3

Authentication functions:MAC,Hash function, Security of hash function and MAC,MD5,SHA,HMAC, CMAC, Digital signature and authentication protocols, DSS,EI Gamal – Schnorr.

Module-4

Authentication applications: Kerberos & X.509 Authentication services Internet Firewalls for Trusted System: Roles of Firewalls , Firewall related terminology-,Types of Firewalls ,Firewall designs, Intrusion detection system , Virus and related threats, Countermeasures , Firewalls design principles ,Trusted systems, Practical implementation of cryptography and security.

Module-5

Quantum Cryptography and Quantum Teleportation: Heisenberg uncertainty principle, polarization states of photons, quantum cryptography using polarized photons, local vs. nonlocal interactions, entanglements, EPR paradox, Bell's theorem, Bell basis, teleportation of a single qubit theory and experiments.

Course outcomes:

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

- Understand OSI security architecture and classical encryption techniques.
- Acquire fundamental knowledge on the concepts of finite fields and number theory.
- Understand various block cipher and stream cipher models.
- Describe the principles of public key cryptosystems, hash functions and digital signature.
- Compare various Cryptographic Techniques
- Design Secure applications
- Inject secure coding in the developed applications

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- 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 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.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
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.	Quantum Computation and Quantum Information	Michel A Nielson	Cambridge University press	10th Anniversary edition
Reference Books				
1	Cryptography and Network Security	Behrouz A Forouzan, Debdeep Mukhopadhyay	Mc-GrawHill	3rd Edition, 2015
2	Applied Cryptography and Network Security	Damien Vergnaud and Michel Abdalla	7th International Conference, ACNS 2009, Paris-Rocquencourt,	June 2-5, 2009, Proceedings

			France	

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -II

NETWORK SECURITY AND NETWORK PROGRAMMING LABORATORY

Course Code	**20SCRL26**	CIE Marks	40
Teaching Hours/Week (L:P:S)	0:4:0	SEE Marks	60
Credits	02	Exam Hours	03

PART A: Network Security Laboratory

List of Experiments

1. Apply the RSA algorithm on a text file to produce cipher text file.
2. Develop a mechanism to setup a security channel using Diffie-Hellman Key Exchange between client and server.
3. Implement secure hash algorithm for Data Integrity. Implement MD5 and SHA-1 algorithm, which accepts a string input, and produce a fixed size number - 128 bits for MD5; 160 bits for SHA-1, this number is a hash of the input. Show that a small change in the input results in a substantial change in the output
4. Write a TCP client/server program in which client sends three numbers to the server in a single message. Server returns sum, difference and product as a result single message. Client program should print the results appropriately.

Note: Python / JAVA as programming language

Mini Project: Formulate a problem and using the skills learnt from the course and laboratory exercise solve.

Course outcomes:

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

- Implement various encryption techniques
- Generate and test message digest
- Perform inter-process communication between two machines in a network

Conduction of Practical Examination:

All laboratory experiments (nos) aretobeincludedforpracticalexamination.

Studentsto pick one experimentfrom **each part and execute both**

Strictlyfollow theinstructions as printed on the cover page of answer script for breakup of marks

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

Textbook/ Textbooks

Sl No	**Title of the book**	**Name of the Author/s**	**Publisher Name**	**Edition and year**
1				

Reference Books

1				

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -III

MACHINE LEARNING TECHNIQUES

Course Code	**20SCR31,** 20SFC254, 20SSE334, 20LNI322, 20SCE321, 20SCN324, 20SIT322, 20SAM21	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

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

Module -2

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

Module – 3

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

Module-4

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

Module-5

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

Course outcomes:

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

- Choose the learning techniques with this basic knowledge.
- Apply effectively neural networks and genetic algorithms for appropriate applications.
- Apply bayesian techniques and derive effectively learning rules.
- Choose and differentiate reinforcement and analytical learning techniques
-

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- 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 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.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Machine Learning	Tom M. Mitchell	McGraw-Hill Education	2013

Reference Books

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Introduction to Machine Learning	EthemAlpaydin	PHI Learning Pvt. Ltd	2nd Ed., 2013
2	The Elements of Statistical Learning	T. Hastie, R. Tibshirani, J. H. Friedman	Springer	1st edition, 2001

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -III

OPERATING SYSTEM SECURITY

Course Code	**20SCR321,** 20SFC22	CIE Marks	40
Teaching Hours/Week (L:P:S)	3:0:2	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

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

Module 2

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

Module 3

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

Module 4

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

Module 5

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

Case study: Building secure OS for Linux: Linux security modules, security enhanced Linux.

Course outcomes:

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

- Gain the knowledge of fundamental concepts and mechanisms for enforcing security in OS.
- Analyze how to build a secure OS by exploring the early work in OS.
- Identify and compare different formal security goals and variety of security models proposed for development of secure operating systems.
- Interpret architectures of various secure OS and retrofitting security feature on existing commercial OS's.
- Shows variety of approaches applied to the development & extension services for securing operating systems.

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- 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 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.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Operating system security	Trent Jaeger	Morgan & Claypool Publishers	2008

Reference Books

1	Guide to Operating system Security	Michael Palmer	Thomson	

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -III

DATA MINING & DATA WAREHOUSING

Course Code	**20SCR322,** 20SFC251, 20SIT23, 20SSE241, 20SIS331	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Introduction and Data Preprocessing :Why data mining, What is data mining, What kinds of data can be mined, What kinds of patterns can be mined, Which Technologies Are used, Which kinds of Applications are targeted, Major issues in data mining .Data Preprocessing: An overview, Data cleaning, Data integration, Data reduction, Data transformation and data discretization.

Module -2

Data warehousing and online analytical processing: Data warehousing: Basic concepts, Data warehouse modeling: Data cube and OLAP, Data warehouse design and usage, Data warehouse implementation, Data generalization by attribute-oriented induction,

Module – 3

Classification: Basic Concepts: Basic Concepts, Decision tree induction, Bays Classification Methods, Rule-Based classification, Model evaluation and selection, Techniques to improve classification accuracy

Module-4

Cluster Analysis: Basic concepts and methods: Cluster Analysis, Partitioning methods, Hierarchical Methods, Density-based methods, Grid-Based Methods, Evaluation of clustering.

Module-5

Data mining trends and research frontiers: Mining complex data types, other methodologies of data mining, Data mining applications, Data Mining and society.

Course outcomes:

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

- Demonstrate Storing voluminous data for online processing, Preprocess the data for mining applications
- Apply the association rules for mining the data
- Design and deploy appropriate classification techniques
- Cluster the high dimensional data for better organization of the data
- Discover the knowledge imbibed in the high dimensional system

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- 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 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.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Data Mining Concepts and Techniques	Jiawei Han, Micheline Kamber, Jian Pei	ELSEVIER	3rd edition 2012

Reference Books

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -III

SPEECH PROCESSING

Course Code	**20SCR323,** 20SCS333 20SAM334	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Introduction, Fundamentals of Digital Speech Processing

Module-2

Digital models for the speech signals, Time domain models for speech processing

Module-3

Digital representation of the speech waveform, short term Fourier analysis

Module-4

Homomorphic speech processing, Linear predictive coding of speech: Introduction, Basic principles of LP analyse, Computation of gain for the model, solution of LPC equation, Comparison between the methods of solution of the LPC analysis equation, the prediction error signal.

Module-5

Linear predictive coding of speech: Frequency domain interpretation of LP analysis, Relation of LP analysis, Relations between various speech parameters, applications, Digital speech for man machine communication by voice

Course outcomes:

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

- Explain the fundamentals of speech processing
- Summarize the models of speech processing
- Infer the linear predictive coding
- Illustrate the application of speech processing

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- 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 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.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Digital Processing of Speech Signals	Lawrence R. Rabiner , Ronald W. Schafer	Pearson	

Reference Books

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -III

TRENDS IN ARTIFICIAL INTELLIGENCE AND SOFT COMPUTING

Course Code	**20SCR324,** 20SIT323	CIE Marks	40
TeachingHours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Role of AI in Engineering, AI in daily life, Intelligence and AI, Different Task Domains of AI, History and Early Works of AI, History of AI, Programming Methods, Limitaions of Ai, Agent, Performance Evaluation, Task environment of an Agent, Agents Classification, Agent Architecture

Logic Programming, Logic Representation, Propositional Logic, Predicate Logic and Predicate Calculus, Horn Clauses, Well formd Formula, Computable functions and predicate, Quantifiers, Universe of discourse, Applications of Predicate Logic, Unification,Resolution, Conjuctive Normal Form, conversion to normal form or clausal form

Module 2

Fundamental Problem of Logic: Logic Inadequacy: FundamentaProblem of Logic-Monotonicity wuith "Flying Penguin" example, General disadvantage of monotonicity property in logic , logic in search space problem, logic in decidability and Incompleteness, Logic in Uncertainty Modelling,

Knowledge representation: Knowledge, Need to represent knowledge, Knowledge representation with mapping scheme, properties of a good knowledge base system, Knowledge representation issues, AND-OR graphs, Types of knowledge, Knowledge representation schemes, , semantic nets, Frames, conceptual graphs, conceptual dependence theory, script, weak and strong slot filler.

Reasoning: Types of Reasoning, Methods of reasoning, Application of Reasoning, Forward and Backward Reasoning

Module 3

Search Techniques: Search, Representation techniques, Categories of Search, Disadvantage of state space search, Issues in design of search programs, General Search examples, Classification of search diagram representation, Hill climbing method and Hill climbing search ,Simulates Annealing, Best-First Search, Branch and Bound Search, A* search

Game Playing: Two player games, Minmax Search, Complexity of Minmax algorithm, Alpha-Beta Pruning

Planning: Necessity of planning, Components of Planning, Planning Agents, Plan-gererating schemes, Algorithm for planning, Planning Representation with STRIPS, BlOCKS WORLD, difficulties with planning

Module 4

Fuzzy Sets and Uncertainties: Fuzzy set and fuzzy logic, set and fuzzy operators, , Extended fuzzy operations, Fuzzy relations, Properties of fuzzy relations, Fuzzy system and design, Linguistic hedges, Syntax for IF and Then rules, , Types of fuzzy rule based system, Fuzzy linguistic controller, Fuzzy Inference, Graphical techniques of Inference, How, Fuzzy logic is used, Fuzzification, De-fuzzification. Unique features of Fuzzy Logic, Application of Fuzzy Logic, Fuzzy logic uncertainty and probability, Advantages and Limitations of Fuzzy logic and Fuzzy Systems

Module 5

Advancement of AI: Expert System, Expert System structure, Knowledge acquisition, Knowledge representation, Inference control mechanism, User interface, Expert System Shell, Knowledge Representation, Inference Mechanism, Developer Interface and User Interface, Characteristics of Expert system, Advantages of an expert system, Production System, Artificial Neural Networks, : Characteristics of Neural Networks, Architecture of neural networks, Types of neural networks, Application of neural networks.

Course outcomes:

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

- Design intelligent agents for problem solving, reasoning, planning, decision making, and learning. specific design and performance constraints, and when needed, design variants of existing algorithms.

- Apply AI technique to current applications.
- Apply Problem solving, knowledge representation, reasoning, and learning techniques to solve real world problems
- Design and build expert systems for various application domains.
- Apply Soft Computing techniques such as neural networks, fuzzy logic to solve problems in various application domains

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- 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 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.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Artificial Intelligence and Softcomputing for Beginners	Anindita Das Battacharjee	Shroff Publishers	2nd edition

Reference Books

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Artificial Intelligence	Elaine Rich,Kevin Knight, Shivashanka B Nair	Tata CGraw Hill	3rd edition. 2013
2	Artificial Intelligence A Modern Approach	Stuart Russel, Peter Norvig	Pearson	3rd edition 2013
3	Neural Networks, Fuzzy Logic and Genetic	S. Rajasekaran, G. A. Vijayalakshmi PaiAlgorithms	PHI publication	
4	Principles of Artificial Intelligence	Nils J. Nilsson	Elsevier	

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -III

MANAGING BIG DATA

Course Code	**20SCR331,** 20SFC331, 20SIT31, 20LNI251, 20SCE21, 20SIS332	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Meet Hadoop: Data!, Data Storage and Analysis, Querying All Your Data, Beyond Batch, Comparison with Other Systems: Relational Database Management Systems, Grid Computing, Volunteer Computing Hadoop Fundamentals MapReduce A Weather Dataset: Data Format, Analyzing the Data with Unix Tools, Analyzing the Data with Hadoop: Map and Reduce, Java MapReduce, Scaling Out: Data Flow, Combiner Functions, Running a Distributed MapReduce Job, Hadoop Streaming

The Hadoop Distributed Filesystem The Design of HDFS, HDFS Concepts: Blocks, Namenodes and Datanodes, HDFS Federation, HDFS High-Availability, The Command-Line Interface, Basic Filesystem Operations, Hadoop Filesystems Interfaces, The Java Interface, Reading Data from a Hadoop URL, Reading Data Using the FileSystem API, Writing Data, Directories, Querying the Filesystem, Deleting Data, Data Flow: Anatomy of a File Read, Anatomy of a File Write.

Module -2

YARN Anatomy of a YARN Application Run: Resource Requests, Application Lifespan, Building YARN Applications, YARN Compared to MapReduce, Scheduling in YARN: The FIFO Scheduler, The Capacity Scheduler, The Fair Scheduler, Delay Scheduling, Dominant Resource Fairness

Hadoop I/O Data Integrity, Data Integrity in HDFS, LocalFileSystem, ChecksumFileSystem, Compression, Codecs, Compression and Input Splits, Using Compression in MapReduce, Serialization, The Writable Interface, Writable Classes, Implementing a Custom Writable, Serialization Frameworks, File-Based Data Structures: SequenceFile

Module – 3

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

How MapReduce Works Anatomy of a MapReduce Job Run, Job Submission, Job Initialization, Task Assignment, Task Execution, Progress and Status Updates, Job Completion, Failures: Task Failure, Application Master Failure, Node Manager Failure, Resource Manager Failure, Shuffle and Sort: The Map Side, The Reduce Side, Configuration Tuning, Task Execution: The Task Execution Environment, Speculative Execution, Output Committers

Module-4

MapReduce Types and Formats: MapReduce Types, Input Formats: Input Splits and Record,s Text Input, Binary Input, Multiple Inputs, Database Input (and Output) Output Formats: Text Output, Binary Output, Multiple Outputs, Lazy Output, Database Output,

Flume Installing Flume, An Example,Transactions and Reliability, Batching, The HDFS Sink, Partitioning and Interceptors, File Formats, Fan Out, Delivery Guarantees, Replicating and Multiplexing Selectors, Distribution: Agent Tiers, Delivery Guarantees, Sink Groups, Integrating Flume with Applications, Component Catalog

Module-5

Pig Installing and Running Pig, Execution Types, Running Pig Programs, Grunt, Pig Latin Editors, An Example: Generating Examples, Comparison with Databases, Pig Latin: Structure, Statements, Expressions, Types, Schemas, Functions, Data Processing Operators: Loading and Storing Data, Filtering Data, Grouping and Joining Data, Sorting Data, Combining and Splitting Data.

Spark An Example: Spark Applications, Jobs, Stages and Tasks, A Java Example, A Python Example, Resilient Distributed Datasets: Creation, Transformations and Actions, Persistence, Serialization, Shared Variables, Broadcast Variables, Accumulators, Anatomy of a Spark Job Run, Job Submission, DAG Construction, Task Scheduling, Task Execution, Executors and Cluster Managers: Spark on YARN

Course outcomes:

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

- Understand managing big data using Hadoop and SPARK technologies
- Explain HDFS and MapReduce concepts
- Install, configure, and run Hadoop and HDFS.
- Perform map-reduce analytics using Hadoop and related tools
- Explain SPARK concepts

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- 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 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.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Hadoop: The Definitive Guide	Tom White	O'Reilley	Third Edition, 2012

Reference Books

1	SPARK: The Definitive Guide	MateiZaharia and Bill Chambers	Oreilly	2018
2	Apache Flume: Distributed Log Collection for Hadoop	. D'Souza and Steve Hoffman	Oreilly	2014

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -III

ANALYSIS OF COMPUTER NETWORKS

Course Code	**20SCR332,** 20SCN331	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Introduction: Two examples of analysis: Efficient transport of packet voice calls, Achievable throughput in an input-queuing packet switch; the importance of quantitative modelling in the Engineering of Telecommunication Networks.

Module -2

Multiplexing: Network performance and source characterization; Stream sessions in a packet network: Delay guarantees; Elastic transfers in a packet network; Packet multiplexing over Wireless networks.

Module – 3

Stream Sessions: Deterministic Network Analysis: Events and processes in packet multiplexer models: Universal concepts; Deterministic traffic models and Network Calculus; Scheduling; Application to a packet voice example; Connection setup: The RSVP approach; Scheduling (continued).

Module-4

Stream Sessions: Stochastic Analysis: Deterministic analysis can yield loose bounds; Stochastic traffic models; Additional notation; Performance measures; Little's theorem, Brumelle's theorem, and applications; Multiplexer analysis with stationary and ergodic traffic; The effective bandwidth approach for admission control; Application to the packet voice example; Stochastic analysis with shaped traffic; Multihop networks; Long-Range-Dependent traffic

Module-5

Adaptive Bandwidth Sharing for Elastic Traffic: Elastic transfers in a Network; Network parameters and performance objectives; sharing a single link; Rate-Based Control; Window-Based Control: General Principles; TCP: The Internet's Adaptive Window Protocol; Bandwidth sharing in a Network.

Course outcomes:

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

- List and classify network services, protocols and architectures, explain why they are layered.
- Implement key Internet applications and their protocols and apply to develop their own applications (e.g. Client Server applications, Web Services) using the sockets API.

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- 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 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.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Communication Networking An Analytical Approach	Anurag Kumar, D. Manjunath, Joy Kuri	Elsevier	2004

Reference Books

1	Broadband Integrated Networks	M. Schwartz	Prentice Hall	1996
2	High Performance Communication Networks	J. Walrand, P. Varaiya	Morgan Kaufmann	2nd Edition, 1999

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -III

NATURAL LANGUAGE PROCESSING

Course Code	**20SCR333,** 20SCS242, 20SCE243, 20SAM23	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

OVERVIEW AND LANGUAGE MODELING: Overview: Origins and challenges of NLP-Language and Grammar-Processing Indian Languages- NLP Applications-Information Retrieval. Language Modeling: Various Grammar- based Language Models-Statistical Language Model.

Module -2

WORD LEVEL AND SYNTACTIC ANALYSIS: Word Level Analysis: Regular Expressions-Finite-State Automata-Morphological Parsing-Spelling Error Detection and correction-Words and Word classes-Part-of Speech Tagging. Syntactic Analysis: Context-free Grammar-Constituency- Parsing-Probabilistic Parsing.

Module - 3

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

Module-4

Evaluating Self-Explanations in iSTART: Word Matching, Latent Semantic Analysis, and Topic Models: Introduction, iSTART: Feedback Systems, iSTART: Evaluation of Feedback Systems, Textual Signatures: Identifying Text-Types Using Latent Semantic Analysis to Measure the Cohesion of Text Structures: Introduction, Cohesion, Coh-Metrix, Approaches to Analysing Texts, Latent Semantic Analysis, Predictions, Results of Experiments. Automatic Document Separation: A Combination of Probabilistic Classification and Finite-State Sequence Modelling: Introduction, Related Work, Data Preparation, Document Separation as a Sequence Mapping Problem, Results. Evolving Explanatory Novel Patterns for Semantically based Text Mining: Related Work, A Semantically Guided Model for Effective Text mining.

Module-5

INFORMATION RETRIEVAL AND LEXICAL RESOURCES: Information Retrieval: Design features of Information Retrieval Systems-Classical, Non classical, Alternative Models of Information Retrieval – valuation Lexical Resources: World Net-Frame Net- Stemmers-POS Tagger- Research Corpora.

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

- Analyse the natural language text.
- Generate the natural language.
- Demonstrate Text mining.
- Apply information retrieval techniques.

Question paper pattern:
The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- 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 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.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Natural Language Processing and Information Retrieval	Tanveer Siddiqui, U.S. Tiwary	Oxford University Press	2008
2	Anne Kao and Stephen R. Potee	Natural LanguageProcessing andText Mining	Springer-Verlag London Limited	2007

Reference Books

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Speech and Language Processing: Anintroduction to Natural Language Processing, Computational Linguistics and SpeechRecognition	Daniel Jurafsky and James H Martin	Prentice Hall	2008 2nd Edition
2	Natural Language Understanding	James Allen	Benjamin/Cummings publishing company	2nd edition, 1995
3	Information Storage and Retrieval systems	Gerald J. Kowalski and Mark.T. Maybury	Kluwer academic Publishers	2000.
4	Natural Language Processing with Python	Steven Bird, Ewan Klein, Edward Loper	O'Reilly Media	2009
5	Foundations of Statistical Natural Language Processing	Christopher D.Manning and Hinrich Schutze	MIT Press	1999

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -III

DEEP LEARNING

Course Code	**20SCR334,** 20SCS31, 20SAM31, 20SIS334	CIE Marks	40
Teaching Hours/Week (L:P:S)	3:0:2	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Machine Learning Basics: Learning Algorithms, Capacity, Overfitting and Underfitting, Hyperparameters and Validation Sets, Estimator, Bias and Variance, Maximum Likelihood Estimation, Bayesian Statistics, Supervised Learning Algorithms, Unsupervised Learning Algorithms, Stochastic Gradient Decent, building a Machine Learning Algorithm, Challenges

Motivating Deep Learning.

Module-2

Deep Feedforward 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.

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.

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

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.

Course outcomes:

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

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

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- 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 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.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Deep Learning	Lan Good fellow and YoshuaBengio and Aaron Courville	MIT Press https://www.deeplearningbook.org/	2016.

Reference Books

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Neural Networks:Asystematic Introduction	Raúl Rojas		1996.
2	Pattern Recognition and machine Learning	Chirstopher Bishop		2007.

M.Tech. in CYBER SECURITY(SCR)

Choice Based Credit System (CBCS) and Outcome Based Education(OBE)

SEMESTER -IV

PROJECT WORK PHASE -2

Course Code	20SCR41	CIE Marks	40
Number of contact Hours/Week	4	SEE Marks	60
Credits	20	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, organisation, 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 instil 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. ■

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 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. ■

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: 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.

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 (30 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. ■