Visvesvaraya Technological University

"Jnana Sangama" Belagavi-590018, Karnataka State, India

Dr. A. S. Deshpande B.E., M.Tech., Ph.D.
Registrar

Phone: (0831) 2498100
Fax: (0831) 2405467

Ref: VTU/BGM/Aca/A9/2020-21/5924

Dated: 9 FEB 2021

CIRCULAR

Subject: Draft Copy of Scheme and Syllabus of M.Tech., in CYBER SECURITY programme regarding...

Reference: Hon'ble Vice-Chancellor's approval dated 08.02.2021

With reference to the subject cited above, a draft copy of the scheme (I to IV semester) and syllabus (I semester) of postgraduate Programme M.Tech., in CYBER SECURITY is uploaded on the University web portal @ **https://vtu.ac.in/en/pg-scheme-syllabus/** for feedback and suggestions.

All the principals of constituent /non-autonomous /autonomous engineering colleges are hereby informed to bring the content of the circular to the notice of all the concerned. Please note that the last date to submit the feedback/suggestions/opinion is 27.02.2021.

Sd/-
REGISTRAR

To,

The Principals of constituent /non-autonomous /autonomous engineering colleges coming under the ambit of the university.

Copy to-

1. To Hon'ble Vice-Chancellor through the secretary to VC for kind information
2. The Registrar (Evaluation) for information and needful.
3. The Regional Directors (I/c) of all the regional offices of VTU for circulation.
4. The Special Officer CNC VTU Belagavi for uploading on VTU website
5. PS to Registrar VTU Belagavi for information
6. All the concerned Special Officer/s and Caseworker/s of the academic section, VTU, Belagavi

9.2.2021

REGISTRAR

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 per Week			Examination				Credits
				Theory	Practical	Skill Development Activities	Duration in hours	CIE Marks	SEE Marks	Total Marks	
				L	P	SDA					
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	02	--	02	03	40	60	100	2
			TOTAL	**17**	**04**	**12**	**21**	**280**	**420**	**700**	**24**

Note: PCC: Professional 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, analyse 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 internship 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.
(iii) Two credit courses are designed for 25 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 Activities	Duration in hours	CIE Marks	SEE Marks	Total Marks	
				L	P	SDA					
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 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: Professional core, PEC: Professional Elective.

Professional Elective 1		Professional Elective 2	
Course Code under 20SCR24X	**Course title**	**Course Code under 20SCR25X**	**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 programme 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/ Mini-Project/ Internship	Skill Development activities	Duration in hours	CIE Marks	SEE Marks	Total Marks	
				L	P	SDA					
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: Professional core, PEC: Professional Elective.											

Professional elective 3		**Professional elective 4**	
Course Code under 20SCR32X	**Course title**	**Course Code under 20SCR33X**	**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	Cyber Crime and Cyber Forensics
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 performance in 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 CYBER SECURITY(SCR)
Choice Based Credit System (CBCS) and Outcome Based Education(OBE)
SEMESTER -I

MATHEMATICAL FOUNDATIONS OF COMPUTER SCIENCE

Course Code	20SCR11	CIE Marks	40
Teaching Hours/Week (L:P:SDA)	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 ttest, χ^2 - test.
(RBT Levels: L1 & L2) (Textbook:3)

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

(1) Linear Algebra and its Applications David C. Lay, Steven R. Lay and J. J. McDonald Pearson Education Ltd 5 th Edition 2015.

(2) Numerical methods for Scientific and Engg. Computation M K Jain, S.R.K Iyengar, R K. Jain New Age International 6 th Ed., 2014

(3) Probability, Statistics and Random Process T. Veerarajan Tata Mc-Graw Hill Co 3 rd Edition 2016

Reference Books

(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 CYBER SECURITY(SCR)
Choice Based Credit System (CBCS) and Outcome Based Education(OBE)
SEMESTER -I

INFORMATION AND NETWORK SECURITY			
Course Code	20SCR12	CIE Marks	40
Teaching Hours/Week (L:P:SDA)	3:0:2	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

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

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. **Web Security Considerations:** Web Security Threats, Web Traffic Security Approaches. **Secure Sockets Layer:** SSL Architecture, SSL Record Protocol, Change Cipher Spec Protocol, Alert Protocol, and shake Protocol, Cryptographic Computations. **Transport Layer Security:** Version Number, Message Authentication Code, Pseudorandom Functions, Alert Codes, Cipher Suites, Client Certificate Types, Certificate Verify and Finished Messages, 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:

1. Analyze the vulnerabilities in any computing system and hence be able to design a security solution.
2. Identify the security issues in the network and resolve it.
3. 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

(1)Cryptography and Network Security William Stallings Pearson 6 th edition

Reference Books

(1) Cryptography and Information Security V K Pachghare PHI 2nd

M.Tech CYBER SECURITY(SCR)
Choice Based Credit System (CBCS) and Outcome Based Education(OBE)
SEMESTER -I

ETHICAL HACKING

Course Code	20SCR13	CIE Marks	40
Teaching Hours/Week (L:P:SDA)	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, Email 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

(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

(2) 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 CYBER SECURITY(SCR)
Choice Based Credit System (CBCS) and Outcome Based Education(OBE)
SEMESTER -I

CLOUD SECURITY

Course Code	20SCR14	CIE Marks	40
Teaching Hours/Week (L:P:SDA)	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

(1) Cloud Security and Privacy, An Enterprise Perspective on Risks and Compliance Tim Mather, SubraKumaraswamy ,ShahedLatifOreilly Media 2009

Reference Books

(1) Securing the Cloud, Cloud Computer Security Techniques and Tactics Vic (J.R.) Winkler Syngress 2011

M.Tech CYBER SECURITY(SCR)
Choice Based Credit System (CBCS) and Outcome Based Education(OBE)
SEMESTER -I

CYBER SECURITY AND CYBER LAW

Course Code	20SCR15	CIE Marks	40
Teaching Hours/Week (L:P:SDA)	3:0:2	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

(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 PrakashTripathi, RitendraGoyal, Praveen Kumar Shukla Dreamtech Press 2015

Reference Books

(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 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:SDA)	0:4:0	SEE Marks	60
Credits	02	Exam Hours	03

Sl. NO	Experiments
1	Wireshark: Experiment to monitor live network capturing packets and analyzing over the live network.
2	LOIC: DoS attack using LOIC.
3	FTK: Bit level forensic analysis of evidential image and reporting the same
4	Darkcomet : Develop a malware using Remote Access Tool Darkcomet to take a remote access over network. 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
Students are allowed to pick one experiment from the list.
Strictly follow the instructions 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

M.Tech CYBER SECURITY(SCR)
Choice Based Credit System (CBCS) and Outcome Based Education(OBE)
SEMESTER-I

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 2full 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. (For the topic Reviewing the literature under module 2), RanjitKumar,SAGE Publications,3rd Edition, 2011.

(3) Study Material (For the topic Intellectual Property under module 5),
Professional Programme Intellectual 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.

*** END OF I SEMESTER ***