COEP Technological University Pune

(A Unitary Public University of Govt. of Maharashtra)

School of Computation Sciences

Department of Computer Science and Engineering

M. Tech in Cyber Security

Curriculum Structure and Detailed Syllabus

w.e.f AY 2024-25

INDEX

Program Educational Objectives (PEOs)

PEO 1. To make students eligible to take up higher studies/research
PEO 2. To build competency among students to take up jobs that require technical expertise and problem solving ability
PEO 3. To inculcate readiness among students for self learning
PEO 4. To build competency among students in applying technology to solve real-life socio-economic problems

Program Outcomes (POs)

The post-graduate students will demonstrate:

PO 1. An ability to independently carry out research /investigation and development work to solve practical problems.
PO 2. An ability to write and present a substantial technical report/document.
PO 3. Students should be able to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program
PO 4. An ability to manage or work in teams with diverse backgrounds in different aspects and communicate effectively
PO 5. Ability of life-long and continuous self learning
PO 6. Ability to carry out collaborative and multidisciplinary work in a professional environment

List of Abbreviations

Abbreviation	Title	No of courses	Credits	% of Credits
PSMC	Program Specific Mathematics Course	1	4	5.88%
PSBC	Program Specific Bridge Course	1	3	4.41%
PCC	Program Core Course	6	18	26.47%
PEC	Program Specific Elective Course	3	9	13.24%
LC	Laboratory Course	5	5	7.35%
VSEC	Vocational and Skill Enhancement Course	2	18	26.47%
OE	Open Elective	1	3	4.41%
SLC	Self Learning Course	2	6	8.82%
AEC	Ability Enhancement Course	1	1	1.47%
MLC	Mandatory Learning Course	2	--	--
CCA	Co-curricular and Extracurricular Activities	1	1	1.47%
	Total	**25**	**68**	**100%**

Semester I

Sr. No.	Course Type	Course Code	Course Name	Teaching Scheme				Credits	Evaluation Scheme (Weightages in %)				
									Theory		Laboratory		
				L	T	P	S		MSE	TA	ESE	ISE	ESE
1	PSMC		Probability, Statistics and Queuing Theory	3	1	0	1	4	30	10	60	-	-
2	PSBC		Algorithms and Complexity Theory	3	0	0	1	3	30	10	60	-	-
3	PCC		Principles of Cryptography	3	0	0	1	3	30	10	60	-	-
4	PCC & LC		Foundation of Cyber Security	3	0	2	1	4	30	10	60	50	50
5	PCC		Secure Coding Practice	3	1	0	1	4	30	10	60	-	-
6	PEC		Program Specific Elective Course-I 1. Advancement in Networking 2. Malware Analysis 3. Python For Cyber Security 4. Courses in association with Industry	3	0	0	1	3	30	10	60	-	-
7	MLC		Research Methodology and Intellectual Property Rights	2	0	0	0	-	30	10	60	-	-
8	MLC		Effective Technical Communication Skills	1	0	0	0	-	30	10	60	-	-
9	AEC		Mini Project/Seminar	0	0	2	1	1	-	-	-	50	50
Total Credits								**22**					

Legends:

L-Lecture, T-Tutorial, P-Practical, S-Self Study, Cr-Credits,

ISE: In-Semester-Evaluation, ESE: End-Semester-Evaluation, MSE: Mid-Semester Evaluation, TA: Teacher's Assessment, CIE: Continuous-Internal-Evaluation

Semester II

Sr. No.	Course Type	Course Code	Course Name	Teaching Scheme				Credits	Evaluation Scheme (Weightages in %)				
									Theory			Laboratory	
				L	T	P	S		MSE	TA	ESE	ISE	ESE
1	OE		Open Elective	3	0	0	1	3	30	10	60	-	-
2	PCC & LC		Network Security	3	0	2	1	4	30	10	60	50	50
3	PCC & LC		Digital Forensics and Data Recovery	3	0	2	1	4	30	10	60	50	50
4	PCC &LC		Wireless and Mobile Security	3	0	2	1	4	30	10	60	50	50
5	PEC		Program Specific Elective –II 1. Blockchain Technology 2. Security in Digital Marketing 3. Cloud Computing and Security 4. Courses in association with Industry	3	0	0	1	3	30	10	60	-	-
6	PEC		Program Specific Elective –III 1. Web Security 2. Internet of Things and Security 3. Vulnerability Assessment & Penetration Testing 4. Courses in association with Industry	3	0	0	1	3	30	10	60	-	-
7	CCA		Liberal Learning Course	0	0	2	2	1	-	-	-	100	-
Total Credits								**22**					

- **The department offers "Data Structures" as Open Elective for students of other departments.**
- **Exit option to qualify for PG Diploma in Cyber Security :**
  - Eight weeks domain-specific industrial internship in the month of June-July after successfully completing first year of the program.

Semester III

Sr. No.	Course Type	Course Code	Course Name	Teaching Scheme				Credits	Evaluation Scheme (Weightages in %)				
									Theory			Laboratory	
				L	T	P	S		MSE	TA	ESE	ISE	ESE
1	SLC		Massive Open Online Course –I	3	0	0	1	3	-	-	100	-	-
2	SLC		Massive Open Online Course –II	3	0	0	1	3	-	-	100	-	-
3	VSEC		Dissertation Phase – I	0	0	12	18	6	-	-	-	40	60
Total Credits								**12**					

Semester IV

Sr. No.	Course Type	Course Code	Course Name	Teaching Scheme				Credits	Evaluation Scheme (Weightages in %)				
									Theory			Laboratory	
				L	T	P	S		MSE	TA	ESE	ISE	ESE
1	VSEC		Dissertation Phase – II	0	0	24	12	12	-	-	-	50	50
Total Credits								**12**					

Semester I

[PSMC] Probability, Statistics and Queuing Theory	
Teaching Scheme Lectures : 3 hrs/week Tutorial :1hr/week Self-Study : 1 hr/week	**Examination Scheme** Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60

Course Outcomes

Students will be able to:

1. Solve problems related to basic probability theory
2. Solve problems related to basic concepts and commonly used techniques of statistics
3. Model a given scenario using continuous and discrete distributions appropriately and estimate the required probability of a set of events
4. Apply theory of probability and statistics to solve problems in domains such as machine learning, data mining, computer networks etc.

Unit 1: Basic Probability Theory **[2 Hrs]**

Probability axioms, conditional probability, independence of events, Bayes' rule, Bernoulli trials.

Unit 2: Random Variables and Expectation **[10 Hrs]**

- Discrete random variables: Random variables and their event spaces, Probability Mass Function, Discrete Distributions such as Binomial, Poisson, Geometric etc., Indicator random variables
- Continuous random variables: Distributions such as Exponential, Erlang, Gamma, Normal etc., Functions of a random variable
- Expectation: Moments, Expectation based on multiple random variables, Transform methods, Moments and Transforms of some distributions such as Binomial, Geometric, Poisson, Gamma, Normal

Unit 3: Stochastic Processes **[6 Hrs]**

Introduction and classification of stochastic processes, Bernoulli process, Poisson process, Renewal processes

Unit 4: Markov chains **[8 Hrs]**

- Discrete-Time Markov chains: computation of n-step transition probabilities, state classification and limiting probabilities, distribution of time between time changes, M/G/1 queuing system
- Continuous-Time Markov chains: Birth-Death process (M/M/1 and M/M/m queues), Non-birth-death processes, Petri nets

Unit 5: Statistical Inference **[8 Hrs]**

Parameter Estimation – sampling from normal distribution, exponential distribution, estimation related to Markov chains, Hypothesis testing.

Unit 6: Regression and Analysis of Variance **[6 Hrs]**

Least square curve fitting, Linear and non-linear regression, Analysis of variance.

Text Books:

1. Ronald Walpole, Probability and Statistics for Engineers and Scientists, Pearson, ISBN-13: 978-

0321629111

References:

1. Kishor Trivedi, Probability and Statistics with Reliability, Queuing, and Computer Science Applications, John Wiley and Sons, New York, 2001, ISBN number 0-471-33341-7

[PSBC] **Algorithms and Complexity Theory**

Teaching Scheme	**Examination Scheme**
Lectures : 3 hrs/week Self-Study : 1 hr/week	Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60

Course Outcomes

Students will be able to:

1. Determine different time complexities of a given algorithm
2. Demonstrate various design techniques using typical algorithms
3. Develop algorithms using various design techniques for a given problem.
4. Formalize and abstract from a given computational task relevant computational problems, reduce problems and argue about complexity classes

Unit-I: Mathematical Foundation **[6 Hrs]**

Growth of functions – Asymptotic notation, Standard notation and common functions, Summations, solving recurrences.

Unit-II: Analysis of Algorithms **[8 Hrs]**

Necessity of time and space analysis of algorithms, Worst case analysis of common algorithms and operations on elementary data structures (e.g. Heapsort), Average case analysis of Quicksort, Amortized analysis.

Unit-III: Standard Design Techniques-I **[6 Hrs]**

Divide and Conquer, Greedy method.

Unit-IV: Standard Design Techniques-II **[8 Hrs]**

Dynamic programming, Graphs and Traversals.

Unit-V: Standard Design Techniques-III **[6 Hrs]**

Backtracking, Branch-and-bound.

Unit VI: Complexity Theory **[6 Hrs]**

Lower-bound arguments, Introduction to NP-Completeness, Reducibility (SAT, Independent Set, 3VC, Subset Su, Hamiltonian Circuit etc), Introduction to approximation algorithms

Text Books:

1. Thomas Cormen, Charles Leiserson, Ronald Rivest and Cliford Stein, “Introduction to Algorithms”, PHI

Reference Books:

1. Horowitz and S. Sahni. “Fundamentals of Computer Algorithms”, Galgotia, 1991

[PCC] **Principles of Cryptography**

Teaching Scheme	**Examination Scheme**
Lectures : 3 hrs/week Self-Study : 1 hr/week	Mid Sem. Exam (MSE) : 30 Marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60 Marks

Course Outcomes:

Students will be able to:

1. Describe the mathematical foundations that support cryptographic algorithms.
2. Explore fundamental concepts in cryptography, including secret-key encryption, public-key cryptography and other algorithms to provide security services.
3. Gain an understanding of modern cryptosystems, their associated algorithms, and cryptanalysis techniques.
4. Recognize critical challenges in information security management and determine the appropriate cryptosystem to design an effective security solution.

Unit 1: Classical Encryption Techniques [8 Hrs]

Classical Encryption Techniques: Symmetric Cipher Model, , Substitution and Transposition Techniques, Cryptanalysis and Brute-Force Attack.

Block Ciphers: Stream Ciphers and block Ciphers, Feistel Cipher structure, Data Encryption Standard (DES), Strength of DES, Block cipher design principles, Tripple DES, Modes of Operation

Unit 2: Public-Key Cryptography [6 Hrs]

Number Theory: Testing for Primality, Chinese Reminder Theorem, Discrete Logarithms

Public Key Cryptography: Principles of public-key cryptosystems

RSA: RSA algorithm, the security of RSA, ElGamal Cryptographic systems

Unit 3: Data Integrity Algorithms [8 Hrs]

Cryptographic Hash Functions: Message Authentication, security requirements of Hash functions, MD5

Message Authentication Code (MAC): requirements for Message Authentication Codes, MACs Based on Hash Functions: HMAC, MACs Based on Block Ciphers: DAA and CMAC

Digital Signature: Elgamal Scheme, DSA (Digital Signature Algorithm), Elliptic Curve Digital Signature Algorithm (ECDSA), Digital Signature Standard (DSS), Security of Digital Signatures.

Unit 4: Key Management and User Authentication [6 Hrs]

Key Management and Distribution: Symmetric Key Distribution, Diffie-Hellman Key Agreement, Distribution of Public Keys, X-509 Certificates.

User Authentication: Remote user Authentication principles, Authentication using Symmetric encryption, Kerberos, Authentication using Asymmetric encryption, Federated Identity Management.

Unit 5: Modern Cryptosystems **[8 Hrs]**

Modern Symmetric Cipher:

Finite Fields: Groups, rings, fields, Modular Arithmetic, Polynomial Arithmetic, Euclid's algorithm, GF(p), GF(2^p)

Advanced Encryption Standard (AES), Evaluation Criteria

Elliptic Curve: Elliptic curve arithmetic, Elliptic curve cryptography, Analog of Diffie-Hellman key exchange, security of ECC.

Quantum Cryptography: Properties of Quantum States, One-time Pad, Quantum Key Distribution (QKD), BB84 Protocol, Security of QKD, Comparison with Classical

Cryptography.

Unit 6: Technology for Secure Computation **[4 Hrs]**

Data Privacy, Searchable Encryption, Homomorphic Encryption, PHE, SHE, FHE, Verifiable Computation, Zero Knowledge Proofs, Multi-Party Computation, Functional Encryption

Topics for Self study **[4 Hrs]**

Matrix operations, Primality Testing, Steganography, RC4 stream cipher, Public Key Infrastructure, SHA-512.

Text Books:

1. William Stallings: Cryptography and Network Security, Pearson 7th edition, 2017
2. Atul Kahate, Cryptography and Network Security, McGraw-Hill, Fourth edition, 2019

References:

1. V K Pachghare: Cryptography and Information Security, PHI 2nd edition, 2015
2. Forouzan, Cryptography and Network Security, Tata McGraw-Hill, 2008
3. Mark A. Will, Ryan K. L. Ko, A Guide to Homomorphic Encryption, The Cloud Security Ecosystem, Elsevier, pp. 101–127, 2015
4. Anne Broadbent, Christian Schaffner, Quantum Cryptography Beyond Quantum Key Distribution, Designs, Codes and Cryptography. Volume 78, Issue 1, pp 351-382, 2016

[PCC & LC] **Foundation of Cyber Security**

Teaching Scheme	**Examination Scheme**
Lectures : 3 hrs/week Labs: 2 hrs/week Self-Study : 1 hr/week	Mid Sem. Exam (MSE) : 30 Marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60 Marks Laboratory: CIE: 50 marks, ESE (Orals): 50 Marks

Course Outcomes:

Students will be able to:

1. Define the need of Cyber Security.
2. Explain the IT act, Application Security vulnerabilities and its mitigation techniques.
3. Demonstrate the knowledge of penetration testing, and social networking security.
4. Analyse the malwares, social networking websites and impact of cyber-crime on ecommerce.

Unit I:Introduction: **[6 Hrs]**

Nature and scope of computer crime, Understanding how cyber criminals and hackers work, Different types of cyber-crimes, Introduction to digital signatures, Cryptography, Digital certificate and public key infrastructure, IT Act., Impact of cyber-crime on e-governance and e-commerce.

Unit II: Malware reverse engineering: **[6 Hrs]**

Overview of malware reverse engineering, Types of malware, Malicious code families, Latest trends in malware analysis, Basic static and dynamic analysis, Malware analysis techniques, Case study.

Unit III: Web application security: **[8 Hrs]**

Introduction to web application security: Attacks, vulnerabilities and mitigation, Client-side security, Server-side security, Application security: HTTPS, HSTS etc., Security engineering: Passwords and their limitations, Attacks on passwords: CAPTCHA, OTP. Advanced security topics: Secure email systems: PGP, SMIME, DKIM, DMARC, DNSSec, SMTP STS etc., Privacy and security for online social networks, Database security, Browser security, Mobile device security.

Unit IV: Ethical hacking and penetration testing: **[8 Hrs]**

Security Technologies: IDS, IPS, Ethical hacking, Penetration testing fundamentals: Reconnaissance, scanning, gaining access, maintaining access, Covering tracks. Concept of Cyberspace & Netizens, Objective & Scope of the Information Technology Act, Comparisons between traditional criminal techniques and Cyber Crime, Public and Private Societies face challenges in addressing cybercrime, Computer Hardware, Networks and Internet: An Introduction.

Unit V: Nature and scope of computer crime, Understanding how cyber criminals and hackers work, types of cyber crime: **[6 Hrs]**

Financial crime, cyber pornography, Forgery, Web Defacement, Data Diddling, Email frauds, Hacking, Tempering, Spamming, Phishing, Spoofing, Pharming, DoS Attacks, Viruses, Trojan, Worm, Malware, Spyware, Botnet etc. Concept of Digital Signatures and Cryptography, Digital Signature Certificate and Public Key Infrastructure. Authorities under the IT Act., Impact of cyber crime on e-governance and e-commerce.

Unit VI: Cyber crime & Computer-based electronic and Digital evidence: **[6 Hrs]**

Indian law perspective, Procedure for search & Seizure, Best practices for cyber crime

Investigations involving the Computer, Internet and Networks : E-mail, Websites, Chatrooms, file sharing, Network Intrusion/Denial of Services, Messages boards, password breaking, keyloggers, IP tracing, etc. Case studies: Cloud security, Operating system security, Security of social networking websites, IoT devices security, E-commerce websites security. [6 Hrs]

Text Books:

[1] Hossein, "Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management", Wiley, Volume 3 edition, ISBN-13: 978-0470323069.

[2] Georgia Weidman, "Penetration testing: A Hands-On Introduction to Hacking", No Starch Press, 2014, ISBN-13: 978-1593275648.

[3] Michael Sikorski and Andrew Honig, " Practical Malware Analysis", No Starch Press, 1st Edition, 2012, ISBN-13: 978-1593272906

Reference Books:

[1] "Practical Internet of Things Security" by Brian Russell, Drew Van Duren, Packt publishing, 2016, ISBN: 9781785889639

[2] T. Mather, S. Kumaraswamy, S. Latif, "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance", O'Reilly Series, 2009, ISBN-13: 978-0596802769.

[3] "Cyberlaw: the Indian perspective"; Pavan Duggal; Saakshar Law Publications, 1st edition, 2002, ISBN: 8189121022, 9788189121020.

[PCC] **Secure Coding Practices**

Teaching Scheme	**Examination Scheme**
Lectures : 3 hrs/week	Mid Sem. Exam (MSE) : 30 Marks
Tutorial :1hr/week	Teachers Assessment (TA) : 10 Marks
Self-Study : 1 hr/week	End Sem. Exam (ESE) : 60 Marks

Course Outcomes:

Students will be able to:

1. Explain what makes code and architecture insecure and vulnerable.
2. Explain what fundamental design principles should be used to make the code secure.
3. Classify various aspects of code security and apply those at various staged of code development.
4. Demonstrate various methodologies for secure software design and coding.
5. Explain and demonstrate various secure design principles while designing an architecture of the system.
6. Apply the learnt concepts at various stages of software development like planning, designing, coding, testing and deployment.

Unit I: Insecure Code and Vulnerabilities [6 Hrs]

Introduction, Broken Access Control, Cryptographic Failures, Injection, Insecure Design, Security Misconfiguration, Vulnerable and Outdated Components, Identification and Authentication Failures, Software and Data Integrity Failures, Security Logging and Monitoring Failures, Server-Side Request Forgery.

Unit II: Secure Coding Fundamentals [7Hrs]

Fundamentals, Buffer Overflows, Race Conditions, Credential Management, Cryptography, SQL Injections, Cross-site Scripting, Error Handling, Exceptions, HTTP, Secure Data Access and Storage, Authorization and Authentication.

Unit III: Secure Programming Design Principles [6Hrs]

Secure Programming Design Principles Overview, Principle of Least Privilege, Fail-Safe Defaults, Principle of Economy of Mechanism, Principle of Complete Mediation, Separation of Privilege Principle, Principle of Open Design, Principle of Least Common Mechanism, Principle of Least Astonishment.

Unit IV: Methodologies for Developing Secure Code [7 Hrs]

Risk analysis and asset vulnerability research, Threat modelling, Static Analysis, Static Application Security Testing,

Unit V: Secure Architecture Design Principles [7 Hrs]

Threat Modeling, Security Parameters, Physical Security, Network Security, Platform Security, Cloud Security, Application and Data Security, Designing Secure Architecture for Banking, Retail Apps, Mobile Apps, IoT Applications, Web Applications, etc.

Unit VI: Security Planning, Design, Implementation, Testing and Deployment [7 Hrs]

Stakeholder requirements, Incident reporting, Secure implementation and integrations, System modifications, Designing Security Policies, Load Testing, Penetration Testing, Deployment, Security Assessment, Security Build, Governance, Disaster recovery and

countermeasures.

Text books:

1. Mark G. Graff and Kenneth R. Van Wyk. “Secure Coding: Principles and Practices” O'Reilly & Associates, Inc
2. C. Warren Axelrod “Engineering Safe and Secure Software Systems”, Artech House Information Security and Privacy.

Reference book:

1. Herbert H. Thompson and Scott G. Chase, “The Software Vulnerability Guide (Programming Series)” Charles River Media.

[PEC] - Advancement in Networking

Teaching Scheme	**Examination Scheme**
Lectures : 3 hrs/week Self-Study : 1 hr/week	Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60

Course Outcomes:

Students will be able to:

1. Capable of understand and implement various routing protocols
2. To have in depth knowledge of socket programming
3. Aware of issues in SAN, SDN and Open Stack Networking

Unit 1: **[06 Hrs]**

Routing Protocols: Distance Vector (RIP), Link State (OSPF), Multicast Routing Protocols:Intradomain and Interdomain, IP Version 6 (IPv6).

Unit 2: **[06 Hrs]**

Transport Layer Introduction: Services and port numbers, TCP, UDP, and SCTP.

Unit 3: **[07 Hrs]**

Sockets Introduction, Elementary TCP Sockets, IO Multiplexing, Socket Options, ElementaryUDP Sockets, elementary SCTP Sockets.

Unit 4: **[07 Hrs]**

Advanced Sockets, Daemon Processes and the Inetd Superserver, Advanced IO Options, Non blocking I/O.

Unit 5: **[08 Hrs]**

Routing Sockets, Broadcasting, Multicasting, Advanced UDP Sockets, Raw Sockets,Out-of-Band Data, Signal Driven IO, IP Options, Data Link Access.

Unit 6: **[06 Hrs]**

Storage and Networking, Software Defined Networks, Open Stack Networking, Neutron.

TEXT BOOKS:

1. Computer Networks: A Systems Approach, 4e. Larry L. Peterson and Bruce S. Davie, Publisher: Morgan Kaufmann; 4 edition (March 22, 2007), ISBN-10: 0123705487, ISBN-13: 978-0123705488
2. UNIX® Network Programming Volume 1, Third Edition: The Sockets Networking API By W. Richard Stevens, Bill Fenner, Andrew M. Rudof , Publisher :Addison Wesley, ISBN : 0-13-141155-1
3. Tom Clark, Designing Storage Area Networks, A Practical Reference for Implementing Fibre Channel and IP SANs, Addison-Wesley Professional, 2nd Edition, 2003.
4. Open Stack Cloud Computing Cookbook, 2nd Edition, Kevin Jackson , Cody Bunch, PacktPublishing, 978-1-78216-758-7

[PEC] Python for Cyber Security	
Teaching Scheme Lectures : 3 hrs/week Self-Study : 1 hr/week	**Examination Scheme** Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60

Course Outcomes:

Students will be able to:

1. Learn python basics and its features
2. Use object oriented programming
3. Use python advanced libraries.
4. Implement packet sniffers, port scanners using socket programming
5. Implement cybersecurity mechanism

Unit 1: Introduction to Python **[8 Hrs]**

Python Basics: Introduction, Why python? Installation of python, setting up the environment, Features of Python, Writing and executing Python program, real time applications of python

Python Syntax: Variables and Data Types, Operators, type casting, Input operation, Comments, Strings and operations on strings flow controls-if, if-else structures, for loop, while loop, break and continue statements, functions, lists and dictionaries

Unit 2: Object Oriented Programming **[8 Hrs]**

Concept of object-oriented programming, creating classes and objects in python, Parameterized and non-parameterized constructors in python, in-built class methods and attributes, Encapsulation, Polymorphism, Inheritance and its types, data abstractions.

Unit 3: Scripting tools and libraries **[8 Hrs]**

Importing and using modules, introduction to os module, ping script, pinging multiple targets, File operations such as creating file, reading a file, writing to the file, Network security related libraries such as Beautiful Soup, YARA, Scapy, Cryptography, Requests, Pylibnet, pymetasploit3

Unit 4: Sockets **[8 Hrs]**

Sockets, Types of sockets, Socket programming using python, network port scanning, packet sniffing using python, TCP packet injection, discovering hidden vulneraries using pymetasploit3, checking SQL injections and cross site scripting, Geolocation Extraction, Real time extraction from social media

Unit 5: Cybersecurity **[8 Hrs]**

Environment requirement, the MITRE ATT&CK and Shield frameworks, Active scanning, search open technical databases, valid accounts, replication through removable media, boot or logon AutoStart execution, boot or logon initialization scripts, hijack execution flow, Impair defenses, hide artifacts,

Unit 6: Reconnaissance and accessing credentials **[8 Hrs]**

Performing reconnaissance on target environment, establishing command and control channels, collecting sensitive data such as user credentials on the system, defensive python for detection of suspicious connections, account discovery, file and directory discovery

Text Books:

1. Howard E. Potson: Python for Cybersecurity: Using Python for Cyber offense and Defense, John Wiley
2. Justin Seitz, Tim Arnold: Black Hat Python: Python programming for Hackers and Pentesters, 2nd Edition, no starch press

[MLC] Research Methodology and Intellectual Property

Teaching Scheme	**Examination Scheme**
Self-Study :2 hrs/week	Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60

Course Outcomes (COs):

Student will be able to

1. Understand research problem formulation and approaches of investigation of solutions for research problems
2. Learn ethical practices to be followed in research
3. Apply research methodology in case studies
4. Acquire skills required for presentation of research outcomes (report and technical paper writing, presentation etc.)
5. Infer that tomorrow's world will be ruled by ideas, concept, and creativity
6. Gather knowledge about Intellectual Property Rights which is important for students of engineering in particular as they are tomorrow's technocrats and creator of new technology
7. Discover how IPR is regarded as a source of national wealth and mark of aneconomic leadership in context of global market scenario
8. Study the national & International IP system
9. Summarize that it is an incentive for further research work and investment in R & D, leading to creation of new and better products and generation of economic and social benefits

Unit I: **[5 Hrs]**

Meaning of research problem, Sources of research problem, Criteria Characteristics of a good research problem, Errors in selecting a research problem, Scope and objectives of research problem. Approaches of investigation of solutions for research problem, data collection, analysis,interpretation, necessary instrumentations.

Unit II: **[5 Hrs]**

Effective literature studies approaches, analysis Use Design of Experiments /Taguchi Method to plan a set of experiments or simulationsor build prototype Analyze your results and draw conclusions or Build Prototype, Test and Redesign

Unit III: **[5 Hrs]**

Plagiarism, Research ethics Effective technical writing, how to write report, Paper. Developing a Research Proposal, Format of research proposal, a presentation and assessment bya review committee

Unit IV: **[4 Hrs]**

Introduction to the concepts Property and Intellectual Property, Nature and Importance of Intellectual Property Rights, Objectives and Importance of understanding Intellectual PropertyRights

Unit V: **[7 Hrs]**

Understanding the types of Intellectual Property Rights: -Patents-Indian Patent Office and its Administration, Administration of Patent System – Patenting under Indian Patent Act , PatentRights and its Scope, Licensing and transfer of technology, Patent information and database. Provisional and Non Provisional Patent Application and Specification, Plant Patenting, Idea Patenting, Integrated Circuits, Industrial Designs, Trademarks (Registered

and unregistered trademarks), Copyrights, Traditional Knowledge, Geographical Indications, Trade Secrets, Case Studies

Unit VI: **[4 Hrs]**

New Developments in IPR, Process of Patenting and Development: technological research, innovation, patenting, development, International Scenario: WIPO, TRIPs, Patenting under PCT

Reference Books:

1. Aswani Kumar Bansal : Law of Trademarks in India
2. B L Wadehra : Law Relating to Patents, Trademarks, Copyright,
    a. Designs and Geographical Indications.
3. G.V.G Krishnamurthy : The Law of Trademarks, Copyright, Patents and
    a. Design.
4. Satyawrat Ponkse: The Management of Intellectual Property.
5. S K Roy Chaudhary & H K Saharay : The Law of Trademarks, Copyright, Patents
6. Intellectual Property Rights under WTO by T. Ramappa, S. Chand.
7. Manual of Patent Office Practice and Procedure
8. WIPO : WIPO Guide To Using Patent Information
9. Resisting Intellectual Property by Halbert ,Taylor & Francis
10. Industrial Design by Mayall, Mc Graw Hill
11. Product Design by Niebel, Mc Graw Hill
12. Introduction to Design by Asimov, Prentice Hall
13. Intellectual Property in New Technological Age by Robert P. Merges, Peter S. Menell, Mark A. Lemley

[MLC] Effective Technical Communication

Teaching Scheme	Examination Scheme
Self-Study : 1 hr/week	Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60

Course Outcomes (COs):

Student will be able to

1. Produce effective dialogue for business related situations
2. Use listening, speaking, reading and writing skills for communication purposes and attempt tasks by using functional grammar and vocabulary effectively
3. Analyze critically different concepts / principles of communication skills
4. Demonstrate productive skills and have a knack for structured conversations
5. Appreciate, analyze, evaluate business reports and research papers

Unit I: Fundamentals of Communication **[4 Hrs]**

7 Cs of communication, common errors in English, enriching vocabulary, styles and registers

Unit II: Aural-Oral Communication **[4 Hrs]**

The art of listening, stress and intonation, group discussion, oral presentation skills

Unit III: Reading and Writing **[4 Hrs]**

Types of reading, effective writing, business correspondence, interpretation of technical reportsand research papers

Reference Books

1. Raman Sharma, “Technical Communication”, Oxford University Press.
2. Raymond Murphy “Essential English Grammar” (Elementary & Intermediate) CambridgeUniversity Press.
3. Mark Hancock “English Pronunciation in Use” Cambridge University Press.
4. Shirley Taylor, “Model Business Letters, Emails and Other Business Documents” (seventhedition), Prentise Hall
5. Thomas Huckin, Leslie Olsen “Technical writing and Professional Communications for Non-native speakers of English”, McGraw Hill.

Reference books/paper(s):

1. D.J.C. MacKay, “Information Theory, Inference, and Learning Algorithms”, Cambridge University Press

2. C. E. Shannon, A Mathematical Theory of Communication, Bell Sys. Tech Journ, 1948.(available online)

Web Resources:

1. NPTEL Course (Information Theory and Coding – IIT, Bombay) : http://nptel.ac.in/syllabus/117101053/

2. MIT OpenCourseWare (Information Theory) : http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-441-information-theory-spring-2010/index.htm

[AEC] Mini Project/Seminar	
Teaching Scheme Laboratory: 2 hours/week Self-Study : 1 hr/week	**Examination Scheme** CIE: 50 marks, ESE (Orals): 50 Marks

Course Outcomes (COs):

Student will be able to

1. Create links across different areas of knowledge and develop ideas to apply the problem-solving skills to a project task.
2. Do independent learning, and critical thinking and develop an attitude of innovation.
3. Identify a methodology for solving the project task and apply engineering knowledge to solve it
4. Communicate effectively and present ideas clearly in both written and oral forms.

Guidelines

Each student shall carry out a Mini Project task jointly in constant consultation with an internal guide assigned by the department. The project task may consider product development, prototype development, simulation development, statistical analysis, etc. The guide will continuously assess the progress of the work. Finally, a project report will be submitted as per the norms of avoiding plagiarism and the presentations will be taken.

Semester II

[OE] Data Structures	
Teaching Scheme Lectures : 3 hrs/week Self-Study : 1 hr/week	**Examination Scheme** Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60

Course Outcomes

Students will be able to:

1. Decide appropriate data structures such as B-trees, heaps etc that best suits for solving a real life problem
2. Implement advanced data structures, such as B-trees, multi-way trees, balanced trees, heaps, priority queues, to solve computational problems
3. Analyze the time and space complexity of advanced data structures and their supported operations
4. Compare the time and space tradeoff of different advanced data structures and their common operations

Unit I: **[6 Hrs]**

Review of Basic Concepts: Abstract data types, Data structures, Algorithms, Big Oh, Small Oh, Omega and Theta notations, Solving recurrence equations, Master theorems, Generating function techniques, Constructive induction.

Unit II: **[8 Hrs]**

Advanced Search Structures for Dictionary ADT: Splay trees, Amortized analysis, 2-3 trees, 2-3-4 trees, Red-black trees, Randomized structures, Skip lists, Treaps, Universal hash functions.

Unit III: **[6 Hrs]**

Advanced Structures for Priority Queues and Their Extensions: Binary Heap, Min Heap, Max Heap, Binomial heaps, Leftist heaps, Skewed heaps, Fibonacci heaps and its amortized analysis, Applications to minimum spanning tree algorithms.

Unit IV: **[6 Hrs]**

Data Structures for Partition ADT: Weighted union and path compression, Applications to finite state automata minimization, Code optimization.

Unit V: **[6 Hrs]**

Graph Algorithms: DFS, BFS, Biconnected components, Cut vertices, Matching, Network flow; Maximum-Flow / Minimum-Cut; Ford–Fulkerson algorithm, Augmenting Path

Unit VI: **[8 Hrs]**

Computational Geometry: Geometric data structures, Plane sweep paradigm, Concurrency, Java Threads, Critical Section Problem, Race Conditions, Re-entrant code, Synchronization; Multiple Readers/Writers Problem

Text Books:

- Introduction to Algorithms; 3rd Edition; by by Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein; Published by PHI Learning Pvt. Ltd. ; ISBN-13: 978-0262033848 ISBN-10: 0262033844

- Algorithms; 4th Edition; by Robert Sedgewick and Kevin Wayne; Pearson Education, ISBN-13: 978-0321573513

References:

- Algorithms; by S. Dasgupta, C.H. Papadimitriou, and U. V. Vazirani; Published by Mcgraw-Hill, 2006; ISBN-13: 978-0073523408 ISBN-10: 0073523402
- Algorithm Design; by J. Kleinberg and E. Tardos; Published by Addison-Wesley, 2006; ISBN-13: 978-0321295354 ISBN-10: 0321295358

[PCC & LC] Network Security	
Teaching Scheme Lectures : 3 hrs/week Labs: 2 hrs/week Self-Study : 1 hr/week	**Examination Scheme** Mid Sem. Exam (MSE) : 30 Marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60 Marks Laboratory: CIE: 50 Marks, (Orals): 50 Marks

Course Outcomes:

Students will be able to:

1. Understand security issues related to networking vulnerabilities, firewalls, intrusion detection systems
2. Identify infrastructure components including devices, topologies, protocols, systems software, management and security
3. Design and develop solutions for technical issues related to networking and security problems.
4. Apply foot-printing, scanning, enumeration and similar techniques to discover network and system vulnerabilities
5. Analyze performance and risk factors of enterprise network systems

Unit I: Introduction **[7 Hrs]**

Overview of security in networking, Vulnerabilities in TCP/IP model, Vulnerabilities at Application layer, Transport Layer, Internetwork Layer, Network Access Layer

Unit II: Message Authentication **[7 Hrs]**

Basic concepts, Authentication Methods, Message Digest, Kerberos, X.509 Authentication Service.

Unit: III Digital Certificates and PKI **[7 Hrs]**

Introduction, Algorithms for Digital Signature, Digital Signature Standards Private- Key Management, The PKIX model, public key Cryptography Standards (PKCS).

Unit IV: MAIL and IP Security **[6 Hrs]**

Introduction, Pretty Good Privacy (PGP), MIME, S/MIME, IP Security Architecture, IPsec, IPv4, IPv6, Authentication Header Protocol, Encapsulating Security Payload Protocol, VPN.

Unit V: Web Security **[6 Hrs]**

Introduction, Secure Socket Layer (SSL), Secure Electronic Transaction (SET) Transport Layer Security (TLS), Secure Hyper Text Transfer Protocol (SHTTP)

Unit VI: Firewalls and IDS **[6 Hrs]**

Introduction, Types of Firewalls, Firewall Architectures, Trusted System, Access Control, Intrusion Detection systems, types of IDS, Intrusion Prevention Systems (IPS), Honeypots.

Text books:

1. V. K. Pachghare, “Cryptography and Information Security”, PHI, Second Edition
2. William Stallings, “Cryptography and Network Security, Principles and Practices”, Pearson Education, Third Edition
3. Charlie Kaufman, Radia Perlman and Mike speciner, “Network security, Private communication in a Public World”.

Reference books:

1. Christopher M. King, “Security architecture, design deployment and operations”, Curtis patton and RSA Press.

2. Stephen Northcatt, Leny Zeltser, “INSIDE NETWORK Perimeter Security”, Pearson Education Asia.
3. Robert Bragge, Mark Rhodes, Heith straggberg, “Network Security the Complete Reference”, Tata McGraw Hill Publication.

Web Resources:

1. http://nptel.iitm.ac.in/courses/106105031/
2. http://www.cert.org/
3. http://www.howard.edu/csl/research_crypt.htm
4. http://www.cs.purdue.edu/homes/ninghui/courses/426_Fall10/lectures.html
5. http://www.cs.uwp.edu/staff/lincke/infosec/
6. http://www.cisa.umbc.edu/courses/cmsc/426/fall06/
7. http://www.cs.northwestern.edu/~ychen/classes/cs395-w05/lectures.html
8. http://www.cs.iit.edu/~cs549/cs549s07/lectures.htm

Suggested List of Assignments:

1. Install, Configure and study a Intrusion detection system (IDS).
2. Implementation of different message digest/hashing techniques such as MD5, SHA
3. Implementation of email security using PGP(create yourself a 1024 bit PGP key. Use your name and email address for your key label. Use PGP to verify the signature on this assignment.)
4. Demonstrate the use of honey pots for the implementation of IDS
5. Use the OpenSSL commands to create a CA root certificate, a server certificate, and two or more client certificates
6. Write a client-server package for file transfer. The server will listen on some network port. When it accepts a connection, it immediately starts up SSL. The server verifies that the client's certificate came from the proper CA; that's the authentication used.

[PCC & LC] Digital Forensics and Data Recovery	
Teaching Scheme Lectures : 3 hrs/week Labs: 2 hrs/week Self-Study : 1 hr/week	**Examination Scheme** Mid Sem. Exam (MSE) : 30 Marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60 Marks Laboratory: CIE: 50 Marks, (Orals): 50 Marks

Course Outcomes:

Student will be able to:

1. Explain various computer forensic techniques/phases
2. Demonstrate the knowledge of forensic examination related to Microsoft Windows and Linux artifacts
3. Analyze different disk drives and file systems used in different operating systems
4. Apply various tools during real world forensic investigation

Unit 1: Introduction: **[7 Hrs]**

Overview of Computer Crime, Forensic investigation Process, Types of investigation, Digital Forensic Evidence, Anti-forensics, Computer Forensic Model, Maintaining Professional Conduct, preparing for investigation and conduction, Report Writing, Data recovery, Forensic tools: OSForensics, FTK, WinHex.

Unit 2: Digital Evidence Acquisition: **[7 Hrs]**

Functions, Categorization, Order of Volatility, Admissibility of Evidence**,** Acquisition and seizure of evidence, Chain of Custody, Storage formats, Image Capturing Process, Image Validation, Imaging tools: ProDiscover, Linux dd command.

Unit 3: MS Windows Forensics: **[10 hrs]**

Windows artifacts, Program Execution artifacts, Windows Registry, Structure, Registry Analysis Tools, Taskbar Jump Lists, Automatic Destination, Custom Destination, Jump List Extract tools: Structured Storage Viewer, Windows Event Logging Service, Events Structure, Eventvwr Tool, Volume Shadow Copies, Analysis Tools, Windows Shell Bags, BagMRU keys, Prefetch Files, Windows Shortcut, UserAssist, IconCache.db, Amcache.hve, RunMRU, SRUDB.dat

Unit 4: Windows File Systems: **[10 Hrs]**

Clusters and Sectors, FAT File System, FAT Boot Sector, Interpretation using WinHex, FAT Directories, File Allocation Table, File Slack, New Technology File System (NTFS), Comparison to FAT, NTFSWalker tool, Partition Boot Sector, Boot Sector in WinHex, Master File Table (MFT), MFT File Attributes, Directory Files (Index Nodes), $INDEX_ROOT, NTFS Encrypting File System (EFS), Whole Disk Encryption, NTFS Compressed Files, File Deletion, Recovery Mechanisms.

Unit 5: Linux File System: **[10 Hrs]**

Examining Linux File Structures, Ext4, Superblocks, Directory entries, Inodes, Data blocks, Acquiring file system images using dd, dcfldd, Write blocking options, Mounting images, Leveraging The Sleuth Kit (TSK) and Autopsy, fsslat, mmls, Forensic data from /etc, /usr, /var, /dev, /proc, Timeline Analysis.

Unit 6: Email Forensics: **[4 Hrs]**

Email Structure, working, Email Protocols, Examining email messages, Email Server Examination, Tracing emails, Email Forensics Tools

References:

1. Bill Nelson Amelia Phillips Christopher Steuart, “Guide to Computer Forensics and Investigations”, 4th Edition, Course Technology, Cengage Learning, ISBN-13: 978-1-435-49883
2. Brian Carrier, “File System Forensic Analysis”, Pearson education, 1st Edition, ISBN-13:978-0321268174
3. E. Casey, Handbook of Digital Forensics and Investigation, Academic Press, 1st Edition,2010, ISBN-13: 978-0123742674
4. Dejey, Murugan, Cyber Forensics, Oxford Higher Education, 2018

[PCC & LC] Wireless and Mobile Security

Teaching Scheme	**Examination Scheme**
Lectures : 3 hrs/week Labs: 2 hrs/week Self-Study : 1 hr/week	Mid Sem. Exam (MSE) : 30 Marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60 Marks Laboratory: CIE: 50 Marks, (Orals): 50 Marks

Course Outcomes:

Students will be able to:

1. Gain knowledge on security and privacy topics in wireless and mobile networking
2. Understand the security and privacy problems in the realm of wireless networks and mobile computing
3. Apply proactive and defensive measures to counter potential threats, attacks and intrusions
4. Analyze the various categories of threats, vulnerabilities, and countermeasures in the area of wireless and mobile networking
5. Design secured wireless and mobile networks that optimize accessibility whilst minimizing vulnerability to security risks
6. Research in the field of mobile and wireless security and privacy

Unit1: Introduction [8 Hrs]

Introduction to wireless networks security: Wired vs. wireless network security, Threat categories and the OSI model, Vulnerabilities, Countermeasures, Security architectures. IEEE 802.11 standard security issues: Authentication and authorization mechanisms, Confidentiality and Integrity, pre-RSNA protocols (WEP), RSNA (802.11i), Key management, Threat analysis and case studies. Mobile networks security.

Unit 2: Securing Wireless Networks [6 Hrs]

Overview of Wireless security, Scanning and Enumerating 802.11 Networks, Attacking, 802.11 Networks, Attacking WPA protected 802.11 Networks, Bluetooth Scanning and Reconnaissance, Bluetooth Eavesdropping, Attacking and Exploiting, Bluetooth, Zigbee Security, Zigbee Attacks.

Unit 3: Ad-hoc Network Security [7 Hrs]

Security in Ad Hoc Wireless Networks, Network Security Requirements, Issues, and Challenges in Security Provisioning, Network Security Attacks, Key Management in Adhoc Wireless Networks, Secure Routing in Adhoc Wireless Networks.

Unit 4: Mobile Security [6 Hrs]

Mobile system architectures, Overview of mobile cellular systems, GSM and UMTS, Security architecture & Attacks, Vulnerabilities in Cellular Services, Cellular Jamming, Attacks & Mitigation, Security in Cellular VoIP Services, Mobile application security.

Unit 5: Security in Mobile Platforms [7 Hrs]

Android vs. ioS security model, threat models, information tracking, rootkits, Threats in mobile applications, analyzer for mobile apps to discover security vulnerabilities, Viruses, spywares, and keyloggers and malware detection.

Unit 6: Mobile Commerce Security [6 Hrs]

Reputation and Trust, Intrusion Detection, Vulnerabilities, Analysis of Mobile commerce platform, secure authentication for mobile users, Mobile commerce security, payment methods, Mobile Coalition key evolving Digital Signature scheme for wireless mobile Networks

Text Book:

1. S. Kami Makki, Peter Reiher, Kia Makki, Niki Pissinou, Shamila Makki, "Mobile and Wireless Network Security and Privacy", Springer, ISBN 978-0-387-71057-0, 09-Aug-2007
2. Anurag Kumar, D. Manjunath, Joy Kuri "Wireless Networking" Morgan Kaufmann Publishers, First edition, 2009.

Reference Books:

1. C. Siva Ram Murthy, B.S. Manoj, "Adhoc Wireless Networks Architectures and Protocols",Prentice Hall, ISBN 9788131706885, 2007
2. Noureddine Boudriga, "Security of Mobile Communications", ISBN 9780849379413, 2010.
3. Kitsos, Paris; Zhang, Yan, "RFID Security Techniques, Protocols and System-On-Chip Design ", ISBN 978-0-387-76481-8, 2008.
4. Johny Cache, Joshua Wright and Vincent Liu," Hacking Wireless Exposed: Wireless Security Secrets & Solutions ", second edition, McGraw Hill, ISBN: 978-0-07-166662-6, 2010.

[PEC] - Block-chain Technology

Teaching Scheme	**Examination Scheme**
Lectures : 3 hrs/week Self-Study : 1 hr/week	Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60

Course Outcomes:

Student will be able to

1. Understand what is blockchain and its need, real world problem(s) that blockchain istrying to solve.
2. Understand and describe how blockchain works.
3. Understand the underlying technology of transactions, blocks, proof-of-work, and consensus building.
4. Understand blockchain existence in the public domain (decentralized, distributed) yemaintain transparency, privacy, anonymity, security, immutability, history.

Unit I: Course Introduction [6 Hrs]

Course objectives and outcomes, History of centralized services, trusted third party for transactions, Making a case for a trustless system, Why blockchain, Decentralized transactions, No permission for transactions needed.

Unit II: Histor [6 Hrs]

How and when blockchain/bitcoin started, Milestones on the development of bitcoin, Criticism, ridicule and promise of bitcoin, Sharing economy, Internet of Value.

Unit III: Overview of blockchain technology [6 Hrs]

What is blockchain, Transactions, Blocks, Hashes, Consensus, Verify and confirm blocks.

Unit IV: Hashes and Transactions [7 Hrs]

Hash cryptography, Encryption vs hashing, Recording transactions, Digital signature, Verifying and confirming transactions

Unit V: Blocks and blockchain [7 Hrs]

Hash pointers, Blocks.

Unit VI: Consensus building [7 Hrs]

Distributed consensus, Byzantine generals problem, Proof of work, Writing to the blockchain

Text Books:

- Arvind Narayanan, “Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction” Princeton University Press (July 19, 2016)

Reading Material:

- https://bitcoin.org/bitcoin.pdf.
- http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.
- http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.
- http://chimera.labs.oreilly.com/books/1234000001802/ch02.html.
- http://chimera.labs.oreilly.com/books/1234000001802/ch07.html#_introduction_2.
- http://chimera.labs.oreilly.com/books/1234000001802/ch08.html.

[PEC] - Security in Digital Marketing

Teaching Scheme	Examination Scheme
Lectures : 3 hrs/week Self-Study : 1 hr/week	Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60

Course Outcomes:

Student will be able to

1. Understand the fundamentals of digital marketing technologies and platforms.
2. Identify security risks and vulnerabilities specific to digital marketing.
3. Apply security measures to protect digital marketing assets and campaigns.
4. Implement monitoring and detection mechanisms for identifying security incidents.
5. Develop incident response plans tailored to digital marketing environments.

Unit1: Introduction to Digital Marketing: [6 Hrs]

Digital marketing: Concept, Features, Difference between traditional and digital marketing, moving from traditional to digital Marketing; c Digital Marketing Channels: Intent Based- SEO, Search Advertising; Brand Based Display Advertising.
Key concepts: SEO, SEM, social media marketing, email marketing, etc.

Unit 2: Social Media Marketing and Display Marketing: [8 Hrs]

Building Successful Social Media strategy; Social Media Marketing Channels; Facebook, LinkedIn, YouTube (Concepts and strategies) Display Advertising: Working of Display Advertising; Benefits and challenges; Overview of Display ad Process.; Define- Customer, Publisher, Objectives; FormatBudget, Media, Ad Formats, Ad Copy.

Unit 3: Introduction to Marketing Security (Marsec): [6 Hrs]

Online marketing security, website security threats, preventing online marketing security breaches, WebFX, with real life demo explanation.

Unit 4: Security and Ecurity and privacy issues in Digital Marketing: [8 Hrs]

Privacy in Digital Marketing, Importance of Data Privacy in Marketers, Data Privacy in Marketers, Data Privacy Regulations, Threats in Digital Marketing, Data Breaches, Types of Attacks,Security Tips for Digital Marketers.

Unit 5: Digital Marketing vs Cyber Security: [6 Hrs]

Basics of cybersecurity principles and terminology, Common Cyber Security Threats for Digital Marketing and their Solutions. Search Engine Optimisation (SEO). Website and landing page security vulnerabilities (Cover some practical demo session)

Unit 6: Mobile Marketing Security: [6 Hrs]

How to increase an app's engagement through in-app advertising, creating copies, App store optimization, Increase app installations, Strategizing & planning to increase app installations and promotions *(Cover some practical demo session)*

Test Books:

1. "Digital Marketing For Dummies" by Ryan Deiss and Russ Henneberry

2. "Cbersecurity Essentials" by Charles J. Brooks
3. "Marketing Data Science: Modeling Techniques in Predictive Analytics with Python and R" by Thomas W. Miller

References:

1. Online articles and case studies.
2. Research papers on cybersecurity and digital marketing

[PEC] Cloud Computing and Security

Teaching Scheme	Examination Scheme
Lectures : 3 hrs/week Self-Study : 1 hr/week	Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60

Course Outcomes:

Student will be able to

1. Understand fundamentals of cloud computing architectures based on current standards, protocols, and best practices intended for delivering Cloud based enterprise IT services and business applications.
2. Identify the known threats, risks, vulnerabilities and privacy issues associated with Cloudbased ITservices.
3. Understand the concepts and guiding principles for designing and implementing appropriate safeguards and countermeasures for Cloud based IT services.
4. Understandapproaches to designing cloud services that meets essential Cloud infrastructure characteristics - on - demand computing, shared resources, elasticity and measuring usage.
5. Understand the industry security standards, regulatory mandates, audit policies and compliance requirements for Cloud based infrastructures.

Unit I: Fundamentals of Cloud Computing and Architectural Characteristic [6 Hrs]

What is Cloud computing, Architectural and Technological Influences of Cloud Computing, Cloud deployment models - Public, Private, Community and Hybrid models, Scope of Control - Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Cloud Computing Roles, Risks and Security Concerns.

Unit II: Security Design and Architecture for Cloud Computing [6 Hrs]

Guiding Security design principles for Cloud Computing - Secure Isolation, Comprehensive data protection, End-to-end access control, Monitoring and auditing, Quick look at CSA, NIST and ENISA guidelines for Cloud Security, Common attack vectors and threats.

Unit III: Secure Isolation of Physical & Logical Infrastructure [6 Hrs]

Isolation - Compute, Network and Storage, Common attack vectors and threats, Secure Isolation Strategies - Multitenancy, Virtualization strategies, Inter-tenant network segmentation strategies, Storage isolation strategies.

Unit IV: Data Protection for Cloud Infrastructure and Service [7 Hrs]

Understand the Cloud based Information Life Cycle, Data protection for Confidentiality and Integrity, Common attack vectors and threats, Encryption, Data Redaction, Tokenization, Obfuscation, PKI and Key Management, Assuring data deletion, Data retention, deletion and archiving procedures for tenant data, Data Protection Strategies.

Unit V: Enforcing Access Control for Cloud Infrastructure based Services [7 Hrs]

Understand the access control requirements for Cloud infrastructure, Common attack vectors andthreats, Enforcing Access Control Strategies - Compute, Network and Storage - Authentication and Authorization, Roles-based Access Control, Multi-factorauthentication, Host, storage and network access control options, OS Hardening and minimization, securing remoteaccess, Verified and measured boot, Firewalls, IDS, IPS and honeypots.

Unit VI: Monitoring, Auditing and Management [7 Hrs]

Proactive activity monitoring, Incident Response, Monitoring for unauthorized access, malicious traffic, abuse of systemprivileges, intrusion detection, events and alerts, Auditing – Record generation, Reporting and Management, Tamper-proofing audit logs, Quality of Services, Secure Management - User management, Identity management, Security Information and Event Management.

Text Books:

- Vic (J.R.) Winkler, "Securing The Cloud: Cloud Computing Security Techniques andTactics" (Syngress/Elsevier) - 978-1-59749-592-9.
- Thomas Erl, "Cloud Computing Design Patterns" (Prentice Hall) - 978-0133858563.

Reference Books:

- John R. Vacca, "Cloud Computing Security: Foundations and Challenges" 1st Edition.

[PEC] Web Security

Teaching Scheme	Examination Scheme
Lectures : 3 hrs/week Self-Study : 1 hr/week	Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60

Unit I: Introduction

The Evolution of Web Applications, Common Web Application Functions, Benefits of Web Applications, Web Application Security, Key Problem Factors in Web Security, The New Security Perimeter, The Future of Web Application Security, Core Defense Mechanisms: Handling User Access, Handling User Input, Handling Attackers

Unit II: Web Application Technologies

The HTTP Protocol, Web Functionality, Encoding Schemes, Mapping the Application, Enumerating Content and Functionality, Analyzing the Application

Unit III: Web Authentication

Authentication Technologies, Design Flaws in Authentication and Mechanisms, Implementation Flaws in Authentication, Securing Authentication

Unit IV: Session Management and Access Control

Weaknesses in Token Generation, Weaknesses in Session Token Handling, Securing Session Management, Access Controls: Common Vulnerabilities Attacking Access Controls

Unit V: Attacking Data Stores

Injecting into SQL, NoSQL, XPath and LDAP, Attacking Back-End Components: Injecting OS Commands, Manipulating File Paths, Injecting into XML Interpreters, Injecting into Back-end HTTP Requests, Injecting into Mail Services, Cross-Site Scripting: Varieties of XSS, Findingand Exploiting XSS Vulnerabilities, Preventing XSS Attacks

Unit VI: Attacking Web Application and Architecture

Tiered Architectures, Shared Hosting and Application Service Providers, Attacking the Application Server: Vulnerable Server Configuration, Vulnerable Server Software, Web Application Firewalls

Text books:

1. Dafydd Stuttard, Marcus Pinto "The Web Application Hacker’s Handbook: Finding andExploiting Security Flaws", Second Edition,John Wiley & Sons, Inc.
2. Bryan Sullivan, Vincent Liu - Web Application Security, A Beginner's Guide-McGraw- Hill Osborne Media (2011)

Reference books:

1. Elisa Bertino, Lorenzo Martino, Federica Paci, Anna Squicciarini (auth.) - Security for Web services and service-oriented architectures-Springer-Verlag Berlin Heidelberg (2010)
2. Hadi Nahari, Ronald L. Krutz - Web Commerce Security_ Design and Development- Wiley (2011)

[PEC] **Internet of Things Security**

Teaching Scheme	**Examination Scheme**
Lectures : 3 hrs/week	Mid Sem. Exam (MSE) : 30 marks
Self-Study : 1 hr/week	Teachers Assessment (TA) : 10 Marks
	End Sem. Exam (ESE) : 60

Course Outcomes:

1. Identify and describe the variety of IoT systems architectures, essential components and challenges specific to IoT systems
2. Apply appropriate security mechanisms for IoT to real-world problems.
3. Reflect on the impact of current and future IoT technologies on security and privacy.
4. Interpret information privacy and data protection requirements in regards to IoT products design.

Unit I: [8 Hrs]

Introduction to IoT: - Definition and Characteristics. Web of Things V/s Internet of Things: - Two pillars of the web, architecture standardization for WoT, Platform middleware for IoT, Unified multitier WoT architecture, WoT portals and Business Intelligence. M2M to IoT: M2M Communication, Trends in Information and Communication Technology, Implications for IoT, Barrier and Concern for IoT.

Unit II: [8 Hrs]

IoT Architecture: Building architecture , Main design principles and needed capabilities, An IoT architectural overview. IoT Reference Model: IoT domain model, Information model, Functional model, Communication Model, Security Model. IoT Reference Architecture: Deployment and Operational view.

Unit III: [6 Hrs]

Security Classification and Access Control Data classification (Public and Private), Internet of Things Authentication and Authorization, Internet of Things Data Integrity

Unit IV: [6 Hrs]

Security for IoT: Security Issues, Challenges, Spectrum of security consideration, privacy consideration, Interoperability Issues, Regularity, Legal and Right Issues, A policy based framework for security and Privacy in IOT

Unit V: [6 Hrs]

Attacks and Implementation of Internet of Things Denial of Service, Sniffing, Phishing, DNS Hijacking, Pharming, Defacement, Firmware of the device, Web Application

Dashboard , Mobile Application Used to Control, Configure and Monitor the Devices

Unit VI: **[6 Hrs]**

Security Protocols and Management Firmware of the device, Web Application Dashboard , Mobile Application Used to Control, Configure and Monitor the Devices, Identity and Access Management, Key Management

TEXT BOOKS:

1. Internet of Things : Converging Technologies for smart Environments and Integrated Ecosystems, Dr. Ovidiu Vermesan, Dr. Peter Friess, River Publication.
2. Practical Internet of Things Security. Packt Publishing Limited
3. Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations. CRC Press

REFERENCES:

1. The Internet of Things: An Overview, Understanding the issues and Challenges of More Connected World, Internet Society October 2015.
2. Designing the Internet of Things, Adrian McEwen, Hakim Cassimally.
3. Architecting the Internet of Things, Dieter Uckelmann, Mark Harrison, Florian Michahelles, Springer 2011.
4. Operating System for low end devices in IOT: Survey, Oliver Hahm, Emmanuel Baccelli,Hauke Petersen, Nicolas Tsiftes, Dec 2015, HAL -hal-01245551.
5. Hersent, O., Boswarthick, D., & Elloumi, O. (2015). The Internet of Things: Key Applications and Protocols. Wiley

[PEC] **Vulnerability Assessment and Penetration Testing**

Teaching Scheme	**Examination Scheme**
Lectures : 3 hrs/week Self-Study : 1 hr/week	Mid Sem. Exam (MSE) : 30 marks Teachers Assessment (TA) : 10 Marks End Sem. Exam (ESE) : 60

Course Outcomes:

Students will be able to:

1. Plan a vulnerability assessment and penetration test for a network.
2. Execute a penetration test using standard hacking tools in an ethical manner.
3. Report on the strengths and vulnerabilities of the tested network.
4. Identify legal and ethical issues related to vulnerability and penetration testing.
5. Demonstrate, document, report on, and provide a clear roadmap for remediation of exposed security issues

Unit 1: Fundamentals **[6 Hrs]**

Need for Vulnerability Assessment , Risk prevention , Compliance requirements, The life cycles of Vulnerability Assessment and Penetration Testing : scoping, information gathering, vulnerability scanning, false positive analysis, vulnerability exploitation (Penetration Testing), report generation.

Unit 2: Information Gathering and Scanning **[8 Hrs]**

Scan prerequisites, Scan-based target system admin credentials, Direct connectivity without a firewall, Scanning window to be agreed upon, Backup of all systems including data and configuration, Creating a scan policy as per target system OS and information, Configuring a scan policy to check for an organization's security policy compliance, Gathering information of target systems , Active and Passive information gathering, Social Engineering Attacks, Port scanning tools.

Unit 3: Scan and Vulnerability Analysis **[8 Hrs]**

Scan Result analysis, Report interpretation, Hosts Summary (Executive), Vulnerabilities By Host, Vulnerabilites By Plugin, False positive analysis, Understanding an organizations' environment, Target-critical vulnerabilities, Port scanning tools, Vulnerability analysis: False positives, Risk severity Applicability analysis, Fix recommendations, Vulnerability Exploitation: Metasploit, Buffer overflow, Fuzzing, Advanced binary exploitation: Reverse engineering, Static code analysis.

Unit 4: Vulnerability Management **[8 Hrs]**

Vulnerability Assessment reports, Stages of vulnerability management : Identify, Assess, Remediate, Report, Improve, Monitor, Vulnerability management tools : Nessus, report customization, report automation, audit policies, Compliance reporting, auditing infrastructure, Compliance check for different OS and databases.

Unit 5: Introduction to Penetration Testing [6 Hrs]

Phases of Penetration Testing, methodologies (Black Box/White Box/Fuzz), penetration testing for Software (Operating system, services, application), Hardware, Network, Processes, End-user behaviour, tools used for penetration testing, Virtual box, Configuration, Reading: Sample PenTest Report, Sample test cases or scenarios.

Unit 6: Case Studies and tools [8 Hrs]

Penetration Testing types : Social Engineering Test, Web Application Test, Physical Penetration Test, Network Services Test, Client-side Test, Tools: Nmap, Nessus, Metasploit, Wireshark, OpenSSL, Acunetix, Intruder.

Text Books:

1. Patrick Engebretson, "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy", Publisher: Syngress (2011).
2. Himanshu Kumar, "Learning Nessus for Penetration Testing" Packt Publishing, Birmingham- Mumbai, 2014
3. Steve Manzuik, André Gold,Chris Gatford, "Network Security Assessment from Vulnerability to Patch", Syngress Publishing, Inc., 2007

Reference Books:

1. Vivek Ramachandran, Cameron Buchanan "Kali Linux Wireless Penetration Testing Beginner's Guide", 2015 Packt Publishing.
2. Justin Clarke-Salt "SQL Injection Attacks and Defense" 1st Edition, Syngress Publication
3. Prakhar Prasad "Mastering Modern Web Penetration Testing", October 2016.

Packt Publishing 4. Wolf Halton, Bo Weaver, "Kali Linux 2: Windows Penetration Testing", June 2016 Packt Publishing.

Semester III

[SLC] **Massive Open Online Course – I**	
Teaching Scheme Lectures : 3 hrs/week Self-Study : 1 hr/week	**Examination Scheme** Theory: CIE: 40 Marks ESE: 60 marks

Course Outcomes:

Students will be able to:

1. Acquire new skills or knowledge to enhance their personal and professional development
2. Receive a flexible learning environment, allowing one to study at own pace and convenience
3. Opportunity for lifelong learning
4. Foster collaboration and networking among participants

The students in consultation with the faculty advisor opt for a single course of 12 weeks offered by the NPTEL in the current semester. The students need to register for the examination conducted by the NPTEL. For the students who secured a passing score in the NPTEL examination, the marks obtained for assignments (in 25 marks) will be upscaled to out of 40 marks of CIE and the marks obtained from the certificate examination (in 75 marks) will be downscaled 60 marks of ESE assessments.

[SLC] **Massive Open Online Course – II**

Teaching Scheme	**Examination Scheme**
Lectures : 3 hrs/week	Theory: CIE: 40 Marks
Self-Study : 1 hr/week	ESE: 60 marks

Course Outcomes:

Students will be able to:

1. Acquire new skills or knowledge to enhance their personal and professional development
2. Receive a flexible learning environment, allowing one to study at own pace and convenience
3. Opportunity for lifelong learning
4. Foster collaboration and networking among participants

The students in consultation with the faculty advisor opt for a single course of 12 weeks offered by the NPTEL in the current semester. The students need to register for the examination conducted by the NPTEL. For the students who secured a passing score in the NPTEL examination, the marks obtained for assignments (in 25 marks) will be upscaled to out of 40 marks of CIE and the marks obtained from the certificate examination (in 75 marks) will be downscaled 60 marks of ESE assessments.

[VSEC] Dissertation Phase – I

Teaching Scheme	**Examination Scheme**
Laboratory: 12 hr/week	Theory: CIE: 40 Marks
Self-Study : 18 hr/week	ESE: 50 marks

Course Outcomes:

Students will be able to:

1. Demonstrate how to search the existing literature to gather information about a specific problem or domain.
2. Identify the state-of-the-art technologies and research in the chosen domain, and highlight open problems that are relevant to societal or industrial needs.
3. Evaluate various solution techniques to determine the most feasible solution within given constraints for the chosen dissertation problem.
4. Apply software engineering principles related to requirements gathering and design to produce relevant documentation.
5. Write a dissertation report that details the research problem, objectives, literature review, and solution architecture.
6. Deliver effective oral presentations to communicate the findings and outcomes of the research work.

Guidelines

The dissertation is a year-long project, conducted and evaluated in two phases. It can be carried out either in-house or within an industry as assigned by the department. The project topic and internal advisor (a faculty member from the department) are determined at the beginning of Phase I.

Student is expected to complete the following activities in Phase-I:

1. Literature survey
2. Problem Definition
3. Motivation for study and Objectives
4. Preliminary design / feasibility / modular approaches

Deliverables

1. A report having following details: Abstract, Problem statement, Requirements specification, Literature survey, Proposed solution, High level design description, Plan for implementation and testing in Phase-II
2. A presentation that covers the major points covered in the report.
3. A proof of concept (preferable but not mandatory)

Evaluation

Two independent assessments (Mid-Semester and End-Semester evaluations) will be done:

1. The internal guide will evaluate his/her student for 40 marks
2. A panel of External Examiner(s) and two senior faculty of the department will evaluate the work for 60 marks.

The marks obtained in these two assessments will be combined to get final evaluation out of 100 marks. The course grading, like other courses, will be relative in nature.

The evaluation will take place based on criteria such as literature survey and well-defined project problem statement, proposed high level system design, concrete plan for implementation and result generation, presentation etc.

The panel (external examiner(s) and senior faculty) will provide a report about suggestions/changes to be incorporated during phase-II.

Semester IV

[VSEC] **Dissertation Phase – II**

Teaching Scheme	**Examination Scheme**
Laboratory: 24 hr/week	Theory: CIE: 50 Marks
Self-Study : 12 hr/week	ESE: 50 marks

Course Outcomes:

Students will be able to:

1. Achieve proficiency in the languages, tools, libraries, and technologies used in the dissertation work.
2. Apply project planning principles and techniques to ensure effective and efficient project execution.
3. Demonstrate an understanding of the entire lifecycle of a software product or solution.
4. Produce artifacts such as source code, test plans, and test results based on the dissertation work.
5. Write research paper(s) and a thesis in accordance with publication ethics.
6. Exhibit the presentation skills needed to effectively present the work at various platforms.

Guidelines

Student is expected to complete the following activities in Phase-II:

1. Implementation of the proposed approach in the first stage
2. Testing and verification of the implemented solution
3. Writing of a report and presentation
4. Publish the work done at suitable conference/in a journal

Deliverables

1. Source code (if the project is in-house)
2. Dissertation report that gives overview of the problem statement, literature survey, design, implementation details, testing strategy and results of testing
3. All the artifacts created throughout the duration of dissertation such as requirements specification, design, project plan, test cases etc
4. Presentation based on the dissertation report 5. Research Paper(s) based on the dissertation work

Evaluation

Evaluation will be done in two steps: Mid-Semester evaluation and End-Semester

evaluation.

• Mid-Semester evaluation:
Evaluation will be done by the internal guide and a qualified external examiner The internal guide will evaluate his/her student for 20 marks. External Examiner will provide evaluation for 30 marks

The assessment is done on the criteria such as concrete system design, implementation status and concrete plan for completion of remaining tasks, presentation etc.

The purpose of Mid-Semester evaluation is also to check preparedness of students for the EndSemester evaluation. Examiners may give suggestions for changes/corrections to be incorporated before the final evaluation. If the work done till then may not lead to successful completion of the dissertation in the remaining time, student may be asked to take extension in time to complete the course.

• End-Semester evaluation:
The internal guide and one external examiner will carry out the final evaluation. The guide will provide evaluation for 20 marks and the external examiner for 30 marks.

The assessment will be done based on the criteria such as quality of implementation, result analysis, project outcomes (publications, patent, copyright, contribution to opensource community, participation in project competition etc.), quality of report, presentation etc.

The total assessment of phase-II work is for 100 marks (Mid-Semester evaluation for 50 marks and End-Semester evaluation for 50 marks) and the grading, like other courses, will be relative.