

PUDUCHERRY TECHNOLOGICAL UNIVERSITY

PUDUCHERRY-605014

(A Technological University of Government of Puducherry)



Curriculum and Syllabi

of

M.Tech. in INFORMATION SECURITY

(With effect from Academic year 2020-21)

(Approved in the Board of Studies Meeting held on 30th August 2023)

CURRICULUM

The curriculum of M.Tech. (Information Security) is designed to fulfill the Programme Educational Objectives (PEO) and Programme Outcomes (PO) listed below:

PROGRAMME EDUCATIONAL OBJECTIVES (PEO)

PEO1	Core Competency To acquire a comprehensive knowledge of Information Security and networking concepts and apply for investigation of real world problems.
PEO2	Versatility and Diversification To garner interdisciplinary knowledge for attaining competitive edge and aligning to industrial needs.
PEO3	Research, Innovation and Entrepreneurship To realize the significance of innovation in research and educate the facets of entrepreneurship complemented with ethical attitude and professionalism.
PEO4	Lifelong Learning To emphasize the need to pursue life-long learning and to stay relevant in emerging technology trends.

PROGRAMME OUTCOMES (PO)

PO1	An ability to independently carry out research /investigation and development work to solve practical problems
PO2	An ability to write and present a substantial technical report/document
PO3	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 program
PO4	The ability to work both independently and as a team member encompassing time management and organizational skills.
PO5	A commitment for life-long learning with professional and ethical responsibility

Distribution of Credits among the subjects grouped under various categories:

Courses are grouped under various categories and the credits to be earned in each category of courses are as follows:

Sl.No.	Category	Credits	Course Category Code
1	Programme Core Course	24	PCC
2	Programme Specific Elective Courses	15	PSE
3	Open Elective Courses	03	OEC
4	Professional Activity Courses (Project Work, Seminar)	28	PAC
5	Mandatory Audit Courses	Non Credit	MAC
	Total	70	

Semester Wise Courses and Credits**Semester I**

Course Code	Course	CCC	Periods			Credits
			L	T	P	
CS263	Mathematical Foundations of Information Security	PCC	3	0	0	3
CS264	Advanced Data Structures and Algorithms	PCC	3	0	0	3
CS265	Principles of Information Security	PCC	3	0	0	3
CSZNN	Programme Specific Elective - 1	PSE	3	0	0	3
CSZNN	Programme Specific Elective - 2	PSE	3	0	0	3
CS266	Information Security Laboratory - 1	PCC	0	0	4	2
CS255	Research Methodology and IPR	PCC	2	0	0	2
AD2NN	Audit Course – I	MAC	2	0	0	0
Total			23			19

Semester II

Course Code	Course	CCC	Periods			Credits
			L	T	P	
CS267	Network Security Essentials	PCC	3	0	0	3
CS268	Information Security Standards and Policies	PCC	3	0	0	3
CS269	Ethical Hacking	PCC	3	0	0	3
CSZNN	Programme Specific Elective - 3	PSE	3	0	0	3
CSZNN	Programme Specific Elective - 4	PSE	3	0	0	3
CS270	Information Security Laboratory - 2	PCC	0	0	4	2
CS271	Mini Project and Seminar	PAC	0	0	4	2
AD2NN	Audit Course – II	MAC	2	0	0	0
Total			25			19

Semester III

Course Code	Course	CCC	Periods			Credits
			L	T	P	
CSZNN	Programme Specific Elective - 5	PSE	3	0	0	3
OE2NN	Open Elective	OEC	3	0	0	3
CS272	Dissertation – Phase I	PAC	0	0	20	10
Total			26			16

Semester IV

Course Code	Course	CCC	Periods			Credits
			L	T	P	
CS273	Dissertation – Phase II	PAC	0	0	32	16
Total			32			16

Total Credits: 70

Audit Courses (MAC)

AD201	English for Research Paper Writing
AD202	Disaster Management
AD203	Value Education
AD204	Constitution of India
AD205	Pedagogy Studies
AD206	Stress Management by Yoga

Open Elective Courses (OEC)

OE201	Business Analytics (IT)
OE202	Industrial Safety and Maintenance (ME)
OE203	Operations Research (ME)
OE204	Cost Management of Engineering Projects (CE)
OE205	Composite Materials (PH)
OE206	Waste to Energy (CE)

Programme Specific Electives (PSE)

PSE-1, PSE-2	CSZ28	Soft Computing
	CSZ12	Data Security and Access Control
	CSZ16	Secure Coding
	CSZ17	Malware Analysis and Reverse Engineering
	CSZ18	Machine Learning and Security
	CSZ19	Secure and Resilient Software Development
PSE-3, PSE-4	CSZ20	Data Mining and Knowledge Discovery
	CSZ21	Digital Forensics
	CSZ22	Biometric Security
	CSZ23	Cyber Security Governance
	CSZ24	Cyber Physical Systems
	CSZ25	Intrusion Detection Systems
PSE-5	CSZ26	Security in IoT
	CSZ27	Security in Cloud Computing
	CSZ03	Artificial Intelligence and Intelligent Systems

Department: Computer Science and Engineering				Programme: M.Tech. (Information Security)				
Semester: First				Course Category Code: PCC			Semester Exam Type: TY	
Course Code	Course Name	Periods / Week			Credit	Maximum Marks		
		L	T	P	C	CA	SE	TM
CS263	Mathematical Foundations of Information Security	3	-	-	3	40	60	100
Prerequisite		High School Mathematics and any Programming Language						
Course Outcome	CO1	Understand the Mathematical Concepts and solving the related problems					Understand	
	CO2	Analyse the computational algorithms and Protocols in terms of bit-operations					Analyse	
	CO3	Apply the factorization techniques to factor large numbers and Testing Primality for large numbers					Apply	
	CO4	Construct cryptosystems using Block and Stream ciphers, Knapsack Problem, Discrete Logarithm and Elliptic Curves.					Create	
UNIT-I		Topics in Elementary Number Theory			Periods: 9			
Topics in elementary number theory: Time estimates for doing arithmetic – divisibility and the Euclidean algorithm – Congruences – Linear Congruences, residue classes, Euler’s phi function – Fermat’s Little Theorem – Chinese Remainder Theorem – Applications to factoring – Finite fields – Quadratic Residues and Reciprocity – Legendre Symbol – Jacobi Symbol.							CO1 CO2	
UNIT-II		Simple Cryptosystems			Periods: 9			
Simple Cryptosystems: Enciphering Matrices – Encryption Schemes – Symmetric and Asymmetric. Cryptosystems – Cryptanalysis – Block ciphers – Use of Block Ciphers – Multiple Encryption – Stream Ciphers – Affine cipher – Vigenere, Hill, and Permutation Cipher – Secure Cryptosystem.							CO1 CO4	
UNIT-III		Public Key Cryptosystems			Periods: 9			
Public Key Cryptosystems: The Diffie–Hellman Key Agreement Protocol - RSA Cryptosystem – ElGamal Encryption - Discrete Logarithm – Knapsack problem – ZeroKnowledge Protocols – From Cryptography to Communication Security - Oblivious Transfer.							CO1 CO4	
UNIT-IV		Primality and Factoring			Periods: 9			
Primality and Factoring: Pseudoprimes – the rho method – Format Factorization and Factor Bases – the Continued fraction method – the Quadratic Sieve method.							CO1 CO3	
UNIT-V		Elliptic Curves and Algebraic Geometry			Periods: 9			
Number Theory and Algebraic Geometry: Elliptic curves – basic facts – Elliptic Curve Cryptosystems – Elliptic Curve Primality Test – Elliptic Curve Factorization. (* Theorem Proofs are excluded from all five units in this course of study)							CO1 CO4	
Lecture Periods: 45		Tutorial Periods: -		Practical Periods: -		Total Periods: 45		
Reference Books:								
1. Neal Koblitz, A Course in Number Theory and Cryptography, 2nd Edition, Springer, 2002.								

2. Johannes A. Buchman, Introduction to Cryptography, 2nd Edition, Springer, 2004.
3. Maneses, P. Van Oorschot and S. Vanstone, Hand Book of Applied Cryptography, CRC Press, 2001.
4. Serge Vaudenay, Classical Introduction to Cryptography – Applications for Communication Security, Springer, 2006.
5. Victor Shoup, A Computational Introduction to Number Theory and Algebra, Cambridge University Press, 2005.
6. William Stein, Elementary Number Theory: Primes, Congruences, and Secrets – A Computational Approach, Springer, 2009.

CO – PO Mapping

	PO1	PO2	PO3	PO4	PO5
CO1	3	3	3	1	2
CO2	3	3	3	2	2
CO3	1	3	2	-	-
CO4	3	2	3	2	2
Avg	2.50	2.75	2.75	1.25	1.50

Score: 3 – High; 2 – Medium; 1 – Low

Department: Computer Science and Engineering				Programme: M.Tech.(Information Security)						
Semester: I				Course Category Code: PSE			Semester Exam Type: TY			
Course Code	Course Name			Periods / Week			Credit		Maximum Marks	
				L	T	P	C	CA	SE	TM
CS264	Advanced Data Structures and Algorithms			3	-	-	3	40	60	100
Prerequisite	Nil									
Course Outcome	CO1	Explain the basic data structures and search trees using appropriate examples							Understand	
	CO2	Demonstrate problems on priority queue, heaps, hash tables, set operations, searching /indexing techniques							Understand	
	CO3	Applying appropriate basic algorithmic techniques in solving problems							Apply	
	CO4	Model the problem using appropriate data structures and algorithmic techniques							Apply	
	CO5	Explain algorithms using computational geometry, Np completeness, approximation algorithms, Cryptographic operations, Fast Fourier transform, Linear Programming using appropriate algorithmic techniques							Evaluate	
UNIT-I	Basic Data Structures and Search Trees						Periods: 9			
Algorithm analysis – A mathematical review, case study, Amortized analysis; Basic Data structures– Stacks, Queues, lists, Trees; Binary search trees –Searches and updates, range queries, index based searching-Balanced binary search trees–Ranks and rotations, AVL trees, Red black trees									CO1 CO3	
UNIT-II	Queues, Heaps, Hash Tables and Union-Find Structures						Periods: 9			
Priority queues and heaps – Priority queues, Heaps, Heap sort, Hash tables – Maps, Hash functions, collisions and rehashing, Cuckoo hashing, Universal hashing. Union-Find structures–Union-Find its applications. Multidimensional searching–Range trees, Priority search trees, Quad trees and k-d Trees.									CO2 CO3	
UNIT-III	Fundamental Algorithmic Techniques						Periods: 9			
Algorithmic techniques–The greedy method, Divide and conquer, Dynamic Programming, graphs and traversal. Graph algorithms – Single source shortest paths, Dijkstra’s algorithm, Bellman-Ford algorithm, Shortest paths in directed acyclic graphs, all pairs shortest path, Minimum spanning trees–Properties, Kruskal algorithm, and Prim-Jarnik algorithm. Backtracking and branch and bound techniques.									CO3 CO4	
UNIT-IV	Computational Geometry and Computational Intractability						Periods: 9			
Computational geometry – Operations on Geometric objects, Convex Hulls, Segment Interaction, Finding a Closest Pairs of Points. Computer Intractability-NP completeness – P and NP, NP-Completeness, CNF-SAT and 3SAT, Vertex Cover, Clique, Set cover, Subset sum and knapsack, Hamiltonian cycle and TSP. Approximation algorithms–Themetric Traveling salesman problem, Approximations for covering problems.									CO3 CO4 CO5	

UNIT-V	Fast Fourier Transform and Linear Programming	Periods: 9
The Fast Fourier Transform–Convolution, Primitive roots of unity, The Discrete Fourier Transform, The Fast Fourier Transform Algorithm Linear Programming -Formulating the Problem, The Simplex method, Duality, Application of Linear Programming.		CO3 CO4 CO5
Lecture Periods: 45	Tutorial Periods: -	Practical Periods: -
		Total Periods: 45
Reference Books:		
1. Michael T. Goodrich and Roberto Tamassia, Algorithm Design and Applications, John Wiley & Sons, Inc., USA, 2015 2. Mark Allen Weiss, Data Structures and Algorithm Analysis in C++, 2nd Edition, Pearson, 2004. 3. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein, Introduction to Algorithms, PHI, 3rd Edition, 2010. 4. G. Brassard and P. Bratley, Algorithmics: Theory and Practice, Prentice-Hall, 1997 5. E. Horowitz, S. Sahni and Dinesh Mehta, Fundamentals of Data structures in C++, University Press, 2007. 6. E. Horowitz, S. Sahni and S. Rajasekaran, Computer Algorithms/C++, 2nd Edition, University Press, 2007. 7. Alfred V. Aho, Jeffrey D. Ullman, John E. Hopcroft, Data Structures and Algorithms, Addison Wesley, 2002.		

CO–PO Mapping

	PO1	PO2	PO3	PO4	PO5
CO1	3	3	2	3	3
CO2	3	3	2	3	3
CO3	3	2	3	3	3
CO4	2	2	2	2	2
CO5	2	2	2	2	2
Avg	2.6	2.4	2.2	2.6	2.6

Score: 3–High; 2–Medium; 1–Low

Department: Computer Science and Engineering				Programme: M.Tech.(Information Security)					
Semester: I				Course Category Code: PCC			Semester Exam Type: TY		
Course Code	Course Name		Periods / Week			Credit	Maximum Marks		
			L	T	P			CA	SE
CS265	Principles of Information Security		3	-	-	3	40	60	100
Prerequisite	Nil								
Course Outcome	CO1	Identify the security threats and attacks from both insiders and external sources to an organization.						Apply	
	CO2	Develop an inventory of assets, valuate, prioritize them by applying risk management techniques.						Apply	
	CO3	Design security counter measures for safeguarding the assets from the threats and attacks identified.						Create	
	CO4	Implement information security as a project with periodic maintenance and management.						Apply	
	CO5	Practice security education, training and awareness activities.						Apply	
UNIT I	Introduction to Information Security							Periods : 9	
Introduction- The History of Information Security- Security- CNSS Security Model- Components of an Information System- Balancing Information Security and Access- Approaches to Information Security Implementation- Security in the Systems Development Life Cycle- Security Professionals and the Organization- Information Security: Is It an Art or a Science?								CO4	
UNIT II	Need for Security and Legal Issues in Information’s							Periods : 9	
Introduction- Threats and Attacks- Categories of Threats- Law and Ethics in Information Security- Relevant U.S. Laws- International Laws and Legal Bodies- Ethics and Information Security- Codes of Ethics of Professional Organizations.								CO1	
UNIT III	Security Planning and Managing the Risk							Periods : 9	
Information Security Planning and Governance- Information Security Policy, Standards, and Practices- The Information Security Blueprint- Security Education, Training, and Awareness Program- Continuity Strategies- An Overview of Risk Management- Key Components of Risk Management.								CO2, CO4, CO5	
UNIT IV	Security Technologies							Periods : 9	
Access Control- Firewalls- Intrusion Detection and Prevention Systems- Honey pots, Honey nets, and Padded Cell Systems- Scanning and Analysis Tools.								CO3	
UNIT V	Implementation and Maintenance							Periods : 9	
Information Security Project Management- Technical and Non-Technical Aspects of Implementation- Information Systems Security Certification and								CO4	

Accreditation- Security Management Maintenance Models- Digital Forensics.			
Lecture Periods: 45	Tutorial Periods: -	Practical Periods: -	Total Periods: 45
<u>Reference Books</u>			
1. Michael E Whitman and Herbert J Mattord, "Principles of Information Security", Sixth Edition, 2017. 2. Micki Krause, Harold F. Tipton, "Handbook of Information Security Management", Vol 1-3 CRC Press LLC, 2004.			

CO – PO Mapping

	PO1	PO2	PO3	PO4	PO5
CO1	3	2	3	2	-
CO2	3	2	3	2	-
CO3	3	2	3	2	-
CO4	3	-	3	3	2
CO5	3	-	3	3	2
Avg	3	2.0	3	2.4	2.0

Score: 3 – High; 2 – Medium; 1 – Low

Department: Computer Science and Engineering			Programme: M.Tech.(Information Security)					
Semester: I			Course Category Code: PCC			Semester Exam Type: LB		
Course Code	Course Name	Periods / Week			Credit	Maximum Marks		
		L	T	P		CA	SE	TM
CS266	Information Security Laboratory - I	-	-	4	2	40	60	100
Prerequisite	Programming knowledge and basic concepts of Security.							
Course Outcome	CO1	Identify appropriate cryptographic algorithms to solve specific security problems.						Apply
	CO2	Develop security solutions based on the security needs of the organization.						Apply
	CO3	Apply tools to find vulnerabilities and intrusions in specific organization.						Apply
List of Experiments:								
1. Implement the following Substitution & Transposition Techniques concepts: a) Caesar Cipher b) Playfair Cipher c) Hill Cipher d) Vignère Cipher 2. Implement the RSA algorithm. 3. Implement the following cryptographic algorithms: a) DES b)AES c)SHA-256 4. Implement the Elliptic Curve Cryptography. 5. Implement the Primality Testing.							CO1, CO2	
6. Implement the Diffie Hellman Key Agreement Protocol. 7. Implement the verification of messages using Digital Signature. 8. Configuring S/MIME for E-Mail Communication. 9. Implement password guessing and password cracking. 10. Develop an application which includes authentication, authorization and access control mechanisms.							CO2, CO3	
11. Implement the Intrusion Detection System. 12. Deploy Network Scanning Tools. 13. Deploy Penetration Testing Tools. 14. Implement any OWASP vulnerabilities. 15. Study of OWASP top 10 vulnerabilities in recent year (say 2020).							CO3	
Lecture Periods: -	Tutorial Periods: -		Practical Periods: 60			Total Periods: 60		

CO – PO Articulation Matrix

	PO1	PO2	PO3	PO4	PO5
CO1	3	-	3	2	2
CO2	3	-	3	2	2
CO3	3	-	2	1	1
Avg	3.00	-	2.67	1.67	1.67

Score: 3 – High; 2 – Medium; 1 – Low

Department: Common to all branches				Programme: M. Tech.					
Semester: I				Course Category Code: PCC		Semester Exam Type: TY			
Course Code	Course Name		Periods / Week			Credit	Maximum Marks		
			L	T	P		CA	SE	TM
CE255/ME255/ EC254/CS255/ CH255/EE255/ EI255/IT254	Research Methodology and IPR		2	-	-	2	40	60	100
Prerequisite									
Course Outcomes	CO1	Identify and formulate the research problem for a given engineering domain.							
	CO2	Analyze the literature studies, plagiarism and ethics for the identified research problem.							
	CO3	Develop the effective technical writing and presentation of a research proposal using a tool.							
	CO4	Design and file the copyright of research work for trade as a product in the market.							
	CO5	Apply the research for licensing and technology transfer as a product in world market.							
UNIT I	Introduction					Periods : 6			
Definition 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 instrumentation.								CO1	
UNIT II	Literature Review					Periods : 6			
Effective literature review approaches, literature analysis, avoiding plagiarism, ethics in research, data collection, analysis, interpretation.								CO2	
UNIT III	Technical Writing and Presentation					Periods : 6			
Effective technical writing, how to write report, paper developing a research proposal, format of research proposal, a presentation and assessment by a review committee.								CO3	
UNIT IV	Intellectual Property Rights					Periods : 6			
Intellectual Property – The concept of IPR, Evolution and development of concept of IPR, IPR development process, Trade secrets, utility Models, IPR & Bio diversity, Role of WIPO and WTO in IPR establishments, Right of Property, Common rules of IPR practices, Types and Features of IPR Agreement, Trademark, Functions of UNESCO in IPR maintenance.								CO4	
UNIT V	Patent & Inventions					Periods : 6			

Patents – objectives and benefits of patent, Concept, features of patent, Inventive step, Specification, Types of patent application, process E-filing, Examination of patent, Grant of patent, Revocation, Equitable Assignments, Licenses, Licensing of related patents, patent agents, Registration of patent agents.				CO5
Lecture Periods: 30	Tutorial Periods: -	Practical Periods: -	Total Periods: 30	
Reference Books				
<div>1. C.R.Kothari, ‘Research Methodology Methods & Techniques’, 4th Edn., New Age International Publishers, 2019.</div> <div>2. Catherine Colston, “Principles of Intellectual Property Law”, Cavendish Publishing Ltd, 1999.</div>				

CO – PO Mapping

	PO1	PO2	PO3	PO4	PO5
CO1	3	3	2	3	3
CO2	2	3	3	2	3
CO3	2	3	3	3	2
CO4	3	3	2	3	3
CO5	3	3	3	2	2
Avg	2.6	3	2.6	2.6	2.6

Score: 3 – High; 2 – Medium; 1 – Low

Department: Computer Science and Engineering			Programme: M.Tech. (Information Security)					
Semester: II			Course Category Code:			Semester Exam Type: TY		
Course Code	Course Name	Periods / Week			Credit	Maximum Marks		
		L	T	P			CA	SE
CS267	Network Security Essentials	3	-	-	3	40	60	100
Prerequisite	Nil							
Course Outcome	CO1	Describe various cryptographic techniques used for secure transmission of data						Understand
	CO2	Analyze various network security and web security mechanisms						Apply
	CO3	Develop security solutions based on the security needs of an application						Apply
UNIT I	Introduction					Periods : 9		
Computer Security Concepts, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, A Model for Network Security								CO1
UNIT II	Symmetric and Asymmetric Cryptography					Periods : 9		
Symmetric Encryption Principles, Symmetric Block Encryption Algorithms, Stream Ciphers and RC4, Cipher Block Modes of Operation Public Key Cryptography: Public-Key Cryptography Principles, Public-Key Cryptography Algorithms								CO1, CO3
UNIT III	Message Authentication and Key Distribution					Periods : 9		
Message Authentication : Approaches to Message Authentication, Secure Hash Functions, Message Authentication Codes Key Distribution: Symmetric Key Distribution Using Symmetric Encryption, Kerberos, Key Distribution Using Asymmetric Encryption, X.509 Certificates, Public-Key Infrastructure and Digital Signature								CO1, CO3
UNIT IV	Network Security Applications					Periods : 9		
IP Security Overview , IP Security Policy , Encapsulating Security Payload Transport-Level Security: Web Security Considerations , Secure Socket Layer and Transport Layer Security , Transport Layer Security , HTTPS , Secure Shell (SSH) , Wireless Application Protocol Overview, Wireless Transport Layer Security , WAP End-to-End Security, Electronic Mail Security, Pretty Good Privacy , S/MIME								CO2, CO3
UNIT V	System Security					Periods : 9		
Intruders , Intrusion Detection , Password Management, Malicious Software , Types of Malicious Software, Viruses , Virus Countermeasures , Worms Distributed Denial of Service Attacks, The Need for Firewalls , Firewall Characteristics , Types of Firewalls								CO2, CO3
Lecture Periods: 45	Tutorial Periods: -			Practical Periods: -			Total Periods: 45	
Reference Books								
1. Williams Stallings, Network Security Essentials: Applications and Standards, 6th Edition, Pearson Education, 2016.								
2. Behrouz A. Fourouzan, Cryptography and Network security, 3rd Edition, Tata McGraw-Hill, 2015.								

3. William Stallings, Cryptography and Network Security Principles and Practices, 6th Edition, Prentice Hall, 2013.
4. Charlie Kaufman, Radia Peralman, Mike Speciner, Network Security: Private communication in public world, 2nd edition, Prentice Hall, 2002.

CO – PO Mapping

	PO1	PO2	PO3	PO4	PO5
CO1	2	2	2	1	1
CO2	3	2	3	1	1
CO3	3	2	3	1	1
Avg	2.67	2.00	2.67	1.00	1.00

Score: 3 – High; 2 – Medium; 1 – Low

Department: Computer Science and Engineering				Programme: M.Tech.(Information Security)				
Semester: II				Course CategoryCode: PCC			Semester Exam Type: TY	
Course Code	Course Name	Periods / Week			Credit	Maximum Marks		
		L	T	P			CA	SE
CS268	Information Security Standards and Policies	3	-	-	3	40	60	100
Prerequisite	Nil							
Course Outcome	CO1	Understand the Information Security standards and best practices documents.					Understand	
	CO2	Understand the management, economic, legal and social issues inimplementing the security policies.					Understand	
	CO3	Analyze the policies that address the various information security domains.					Analyze	
	CO4	Design cyber security policies that are enforceable and compliant withthe industry standards and Law.					Apply	
UNIT I	Information Security Standards					Periods : 9		
The Value of Standards and Best Practices Documents, The ISO/IEC 27000 Suite of Information Security Standards, Mapping the ISO 27000 Series to the ISF SGP, NIST Cyber security Framework and Security Documents, The CIS Critical Security Controls for Effective Cyber Defense, COBIT 5 for Information Security, Payment Card Industry Data Security Standard (PCI DSS), ITU-T Security Documents, Using Best Practices and Standards Documents.							CO1	
UNIT II	Information Security Policy Management					Periods : 9		
Business Drivers, Information security policy implementation issues, Types of policies, Industry standard policy frameworks, Best practices for IT Security policy framework creation, Design, Organize, Implement, and Maintain IT Security Policies.							CO2	
UNIT III	Information Security Policies					Periods : 9		
User Domain Policies, Infrastructure Security Policies, Data Classification and handling policies, Risk Management Policies, Incidence Response Team Policies- Business Impact Analysis Policies, Business Continuity Planning Policies, Disaster Recovery Plan Policies							CO3, CO4	
UNIT IV	Implementing an Information Security Policy Framework					Periods : 9		
Security Policy Implementations- Simplified Implementation Process, Target State, Executive Buy-in, Cost, and Impact, Policy Language, Employee Awareness and Training, Information Dissemination—How to Educate Employees, Governance and Monitoring, Best Practices for IT Security Policy Implementations.							CO2	

UNIT V	Policy Enforcement and Compliance	Periods : 9	
Organizational Support for IT Security Policy Enforcement- An Organization's Right to Monitor User Actions and Traffic, Compliance Law, Legal Implications of IT Security Policy Enforcement, Best Practices for IT Security Policy Enforcement, IT Policy Compliance - Creating a Baseline Definition for Information Systems Security, Tracking, Monitoring, and Reporting IT Security Baseline Definition and Policy Compliance, Automating IT Security Policy Compliance, Best Practices for IT Security Policy Compliance Monitoring.			CO2
Lecture Periods: 45	Tutorial Periods: -	Practical Periods: -	Total Periods: 45
<u>Reference Books</u>			
1. William Stallings, Effective Cyber security: A Guide to Using Best Practices and Standards, Addison-Wesley Professional, 2019. 2. Robert Johnson, Security Policies and Implementation Issues, 2nd Edition, Jones & Bartlett Learning, 2014. 3. Douglas J. Landoll, Information Security Policies, Procedures, and Standards: A Practitioner's Reference, 1 edition, Auerbach Publications, 2016.			

CO – PO Mapping

	PO1	PO2	PO3	PO4	PO5
CO1	3	-	3	-	-
CO2	2	-	2	-	-
CO3	2	-	1	2	-
CO4	3	2	3	2	2
Avg	2.5	2	2.25	2	2

Score: 3 – High; 2 – Medium; 1 – Low

Department: Computer Science and Engineering				Programme: M.Tech. (Information Security)						
Semester: II				Course Category Code: PCC			Semester Exam Type: TY			
Course Code	Course Name			Periods / Week			Credit	Maximum Marks		
				L	T	P			CA	SE
CS269	Ethical Hacking			3	-	-	3	40	60	100
Prerequisite	Nil									
Course Outcomes	CO1	Analyse information gathering techniques using Foot printing, scanning and enumeration							Analyse	
	CO2	Assess different tools for such as sensepost, big brother etc for foot printing, AngryIP, Nmap etc for scanning, and Dupmsec, pstools etc for enumeration							Evaluate	
	CO3	Evaluation of social engineering and system hacking methods							Evaluate	
UNIT I	Introduction							Periods : 9		
Introduction to Computer Networks: TCP, IP, ARP. Introduction to Ethical Hacking: Importance of Security-Elements of Security-Phase of an Attack- Hacker Attacks – Hacktivism – Ethical Hackers – Computer Crimes and Implication.									CO1	
UNIT II	Footprinting							Periods : 9		
Introduction – Information gathering methodology – Footprinting tools – WHOIS Tool- DNS Information tool – Locating the network range – E-mail spiders – Locating network activity, Geo Spider, Google Earth – Meta Search Engines.									CO1,CO2	
UNIT III	Scanning and Enumeration							Periods : 9		
Scanning: Introduction – Objectives of scanning – Scanning methodologies – Tools, Live system scanning, Port scanning, Banner Grabbing, Active stack fingerprinting, File extension concealment, Vulnerability scanning, Vulnerability scanning, Network mapping, Proxy, Anonymizer, spoofing tools.Enumeration: Introduction – Techniques – Procedures – Tools, Null session, User account, Null session countermeasure, SNMP, General Enumeration tools.									CO1,CO2	
UNIT IV	Social Engineering							Periods : 9		
Social Engineering: Introduction- Human weakness –Types – Human based social Engineering – Computer based social Engineering – Threats and Defense – Countermeasures- Case studies on Impersonating in Facebook, MySpace and Orkut									CO3	
UNIT V	System Hacking							Periods : 9		
Introduction – Cracking password – Password cracking websites – Instant PDF password remover - Password guessing Algorithms – Password cracking Tools – Countermeasure – Escalating Privileges- Executing Applications – Key loggers and spywares.									CO3	
Lecture Periods: 45		Tutorial Periods: -			Practical Periods: -			Total Periods: 45		
Reference Books										
1. EC- Council, Ethical Hacking and Countermeasures: Attack Phases, Cengage Learning, Second Edition, 2016										
2. EC- Council, Ethical Hacking and Countermeasures: Threats and Defense Mechanisms, Cengage Learning, Second Edition, 2016.										
3. Michael T. Simpson, Hands-On Ethical Hacking and Network Defense, Cengage Learning										

2012.

4. Rafay Baloch, "Ethical Hacking and Penetration Testing Guide", CRC Press, 2014.

CO – PO Mapping

	PO1	PO2	PO3	PO4	PO5
CO1	1	1	3	-	2
CO2	3	1	2	1	2
CO3	3	2	3	2	2
Avg	2.33	1.33	2.66	1.5	2

Score: 3 – High; 2 – Medium; 1 – Low

Department: Computer Science and Engineering				Programme: M.Tech. (Information Security)					
Semester: II				Course Category Code: PCC			Semester Exam Type: LB		
Course Code	Course Name	Periods / Week			Credit	Maximum Marks			
		L	T	P		CA	SE	TM	
CS270	Information Security Laboratory – II	-	-	4	2	40	60	100	
Prerequisite	Nil								
Course Outcomes	CO1	Experiment with various security tools to solve specified problems.					Apply		
	CO2	Evaluate various mechanisms to deal with security vulnerabilities					Evaluate		
	CO3	Develop applications to demonstrate various security issues					Apply		
List of Experiments									
1. Passive information gathering –theHarvester. 2. Active information gathering –Nmap. 3. Detecting Live Systems: a)Switch Miner b) Network Miner 4. Enumerating Systems -SNMP Enumeration. 5. Install and configure Ubuntu in the VM Virtual Box 6. Automated Attack and Penetration Tools: a) OpenVAS b)Nikto 7. Defeating Malware: a. Building Trojans, Rootkit Hunter b. Finding malware 8. Securing Wireless Systems -Acrylic wifi 9. Network analysis tools: a. Angry IP Scanner b. Zenmap c. Wireshark							CO1		
10. Implementation of any one Web attack using Top Ten Vulnerabilities. 11. Implementation of IP spoofing attack. 12. Evaluate Penetration Testing tool: Metasploit and Burpsuite							CO2		
13. Develop an application which should include authentication, authorization and access control mechanism. 14. Develop a web application with secure database using any hashing algorithm. 15. Write a program to generate Password automatically which is easy to remember and calculate the strength the generated password. 16. Write a python program to compare two JSON files and get the duplicate data using key value pair.							CO3		
Lecture Periods:		Tutorial Periods: -		Practical Periods: - 60		Total Periods: 60			

CO – PO Mapping

	PO1	PO2	PO3	PO4	PO5
CO1	3	2	3	2	3
CO2	3	2	3	3	2
CO3	3	3	3	2	3
Avg	3	2.33	3	2.33	2.66

Score: 3 – High; 2 – Medium; 1 – Low

Department: Computer Science and Engineering				Programme: M.Tech.(Information Security)					
Semester: II				Course Category Code: PCC			Semester Exam Type: LB		
Course Code	Course Name	Periods / Week			Credit	Maximum Marks			
		L	T	P		CA	SE	TM	
CS271	Mini Project and Seminar	-	-	4	2	100	-	100	
Prerequisite	Nil								
Course Outcome	CO1	Analyse current challenges faced in the field of Information security				Analyse			
	CO2	Examine advanced security challenges, recent Innovations and technologies to resolve the identified problem.				Analyse			
	CO3	Develop creative thinking in designing viable solutions to information security problems.				Apply			
	CO4	Create appropriate prototypes as part of developing innovative solutions.				Create			
	CO5	Develop effective communication and presentation skills				Apply			
The project work may be either experimental or theoretical in nature, emphasizing on the current trends in Information security. The student is expected to							CO1, CO2, CO3, CO4, CO5		
<ul style="list-style-type: none">Select a research paper on the current issues in the field of information security and perform a detailed study on it.Learn the various approaches to solve the problem identified.Apply the recent tools and techniques to develop a suitable model/prototype of the solution as mini project.Prepare a project report in the specified format for evaluation.Present a seminar on the work done.									
Lecture Periods: -		Tutorial Periods: -		Practical Periods:-		Total Periods: -			

CO – PO Mapping

	PO1	PO2	PO3	PO4	PO5
C01	1	1	1	1	-
C02	3	2	2	2	2
C03	3	2	2	2	3
C04	3	3	3	3	3
C05	3	2	3	3	2
Avg	2.6	2	2.2	2.2	2.5

Score: 3 – High; 2 – Medium; 1 – Low

Semester: III		Course Category Code: PCC			Semester Exam Type: LB			
Course Code	Course Name	Periods / Week			Credit	Maximum Marks		
		L	T	P		CA	SE	TM
CS272	Dissertation-Phase I	-	-	20	10	250	250	500
Prerequisite	Nil							
Course Outcome	CO1	Survey literature references in the field of information security.					Analyse	
	CO2	Build problem analysis skills and generate innovative solutions					Create	
	CO3	Apply necessary tools for the development of components.					Apply	
	CO4	Demonstrate the capability to implement effective security controls and measures.					Understand	
	CO5	Develop effective technical writing, communication and presentation skills.					Apply	
The Dissertation work maybe analytical, experimental, design or combination of both. Phase I the Dissertation work involves the implementation of the existing system. It includes: <ul style="list-style-type: none">• Identification of a suitable problem pertaining to recent issues/ challenges in information security.• In depth literature study of the topic.• Detailed requirement analysis and finalization of the software and hardware requirements.• Preparing a detailed action plan for implementing the solution to the problem.• Detailed Analysis/Modelling/Simulation of the solution to the problem.• Final development of product/process and testing/validation of the results.• Preparation of a report in the specified format for evaluation.								
Lecture Periods: -		Tutorial Periods: -		Practical Periods: -		Total Periods: -		

CO – PO Mapping

	PO1	PO2	PO3	PO4	PO5
--	------------	------------	------------	------------	------------

CO1	3	1	2	1	1
CO2	3	3	3	2	2
CO3	3	2	2	3	1
CO4	3	2	3	1	1
CO5	2	3	3	2	2
Avg	2.8	2.2	2.6	1.8	1.4

Score: 3 – High; 2 – Medium; 1 – Low

Department: Computer Science and Engineering				Programme: M.Tech.(Information Security)					
Semester: IV				Course Category Code: PCC			Semester Exam Type: LB		
Course Code	Course Name		Periods / Week			Credit	Maximum Marks		
			L	T	P		CA	SE	TM
CS273	Dissertation Phase II		-	-	32	16	250	250	500
Prerequisite									
Course Outcome	CO1	Survey literature references in the field of information security.						Analysis	
	CO2	Build problem analysis skills and generate innovative solutions						Create	
	CO3	Evaluate the performance of the work with existing methodologies.						Evaluate	
	CO4	Exhibit effective technical writing, communication and presentation skills.						Apply	
	CO5	Document the work for publication.						Create	
The Dissertation work maybe analytical, experimental, design or combination of both. Phase II the Dissertation work involves the implementation of the proposed system. It includes: <ul style="list-style-type: none">• Identification of a novel approach to solve the problem identified in phase I.• Review and finalization of the approach/methodology identified to solve the problem• Detailed requirement analysis and finalization of the software and hardware requirements.• Preparation of a detailed action plan for implementing the solution to the problem• Detailed Analysis/ Modelling/ Simulation of the solution to the problem.• Final development of product/process, testing/validation of the results and comparison with the existing results.• Preparation of a report in the standard format for evaluation.								CO1, CO2, CO3, CO4, CO5	
Lecture Periods: -		Tutorial Periods: -		Practical Periods: -			Total Periods: -		

CO – PO Mapping

	PO1	PO2	PO3	PO4	PO5
CO1	3	1	2	1	1
CO2	3	3	3	2	2
CO3	3	2	2	1	2
CO4	2	3	3	2	2
CO5	3	3	3	2	3
Avg	2.8	2.4	2.6	1.6	2

Score: 3 – High; 2 – Medium; 1 – Low

PROGRAMME SPECIFIC ELECTIVE COURSES

Department: Computer Science and Engineering			Programme: M.Tech.(Information Security)					
Semester: I			Course Category Code:			Semester Exam Type: TY		
Course Code	Course Name	Periods / Week			Credit	Maximum Marks		
		L	T	P			CA	SE
CSZ28	Soft Computing	3	-	-	3	40	60	100
Prerequisite	Nil							
Course Outcome	CO1	Apply soft computing techniques to solve real world engineering problems.					Apply	
	CO2	Implement nature inspired algorithms to solve combinatorial optimization problems.					Apply	
	CO3	Evaluate the properties of soft computing techniques to develop suitable hybrid solutions.					Evaluate	
	CO4	Demonstrate the use of implementation tools by solving case studies.					Understand	
UNIT I	Introduction to Soft Computing and Fuzzy Logic				Periods : 9			
Introduction - Hard computing vs Soft computing, Constituents of Soft Computing, Hazards of Soft Computing, Fuzzy Logic - Fuzzy Sets, Fuzzy Membership Functions, Operations on Fuzzy Sets, Fuzzy Relations, Operations on Fuzzy Relations, Fuzzy Rules and Fuzzy Reasoning, Fuzzy Inference Systems and Fuzzy Decision Making.							CO1	
UNIT II	Artificial Neural Networks				Periods : 9			
McCulloch Pitt’s Neuron Model, Analogy with biological neurons, Basic principles of ANNs, Types -Single Layer, Multilayer, Competitive, Recurrent, Activation Functions, Learning Paradigms - Supervised and Unsupervised, Perceptron, RBF network, Back Propagation Learning Algorithm, Associative Memory Networks, Kohonen’s Self Organizing Maps, Recurrent Neural network, Third Generation Neural Networks – Convolution Neural Network, Deep Learning Neural Network.							CO1	
UNIT III	Evolutionary Algorithms				Periods : 9			
Introduction, Biological Inspiration, Analogy to Nature’s evolution theory, Genetic Algorithm- Chromosome Encoding Schemes, Population initialization and selection methods, Evaluation function, Genetic operators- Cross over, Mutation, Fitness Scaling, Inversion, Swarm Intelligence Algorithms -Ant Colony Optimization, Particle swarm optimization.							CO2	
UNIT IV	Hybrid Soft Computing Techniques				Periods : 9			
Hybridization Approaches - Neuro -Fuzzy Systems, Neuro-Genetic , Fuzzy- Genetic Systems.							CO3	
UNIT V	Applications and Development Tools				Periods : 9			
Biometric Recognition Systems, Disease Diagnosis Systems, Character Recognition Systems, Soft Computing Implementation issues, Matlab Tool Box for Soft Computing Techniques.							CO4	

Lecture Periods: 45	Tutorial Periods: -	Practical Periods: -	Total Periods: 45
<u>Reference Books</u>			
1. Saroj Kaushik and Sunita Tiwari, "Soft Computing - Fundamentals Techniques and Applications", 1st Edition, McGraw Hill, 2018. 2. Samir Roy, Udit Chakraborty, "Introduction to Soft Computing, Neuro Fuzzy and Genetic Algorithms", Pearson Education, 2013. 3. Anupam Shukla, Ritu Tiwari and Rahul Kala, "Real Time Applications of Soft Computing", CRC Press, 2010. 4. S.N. Sivanandam, S.N. Deepa, "Principles of Soft Computing" , 3 Edition, Wiley India Pvt Ltd, 2019.			

CO – PO Mapping

	PO1	PO2	PO3	PO4	PO5
CO1	3	1	2	1	-
CO2	3	1	3	1	-
CO3	2	2	3	1	-
CO4	3	1	2	1	-
Avg	2.75	1.25	2.5	1.0	-

Score: 3 – High; 2 – Medium; 1 – Low

Department: Computer Science and Engineering				Programme: M.Tech.(Data Science)/M.Tech (Information Security)					
Semester: I				Course Category Code: PSE			Semester Exam Type: TY		
Course Code	Course Name		Periods/Week			Credit	Maximum Marks		
			L	T	P			C A	S E
CSZ12	Data Security and Access Control		3	-	-	3	40	60	100
Prerequisite	Nil								
Course Outcome	CO1	Interpret the various access control mechanisms with their design.						Evaluate	
	CO2	Analyze the different RBAC models and apply them in MLS systems.						Analyze	
	CO3	Interpret the privacy and regulatory issues, standards, and models concerns of the RBAC.						Evaluate	
	CO4	Assess the role engineering plays and use it in enterprises and healthcare applications.						Evaluate	
	CO5	Justify the RBAC in the supporting environment.						Evaluate	
UNIT I	Introduction					Periods:9			
Introduction: Purpose and fundamentals of access control - Brief history – RBAC and the enterprise. Properties, Policies and Models of Access Control: Reference Monitor and Security Kernel – Access control Matrix and Data structure - Discretionary Access Control(DAC)-Non-Discretionary Access Control, Mandatory Access Control(MAC),MAC Policies and models.								CO1	
UNIT II	Role Based Access Control					Periods:9			
CoreRBAC–Role Hierarchies: Inheritance Scheme–Hierarchy structure, SoD and Constraints in RBAS Systems: Types of SoD– SoD in real systems – Temporal Constraints in RBAC-Comparing RBAC to DAC and MAC: Enforcing DAC/MAC using RBAC Implementing RBAC in MLS Systems.								CO2	
UNIT III	Privacy and Regulatory Issues					Periods:9			
Privacy Requirement and Access control Framework – Integrate Privacy Policy support –RBAC and regulatory compliance. RBAC Standards and Profiles: The ANSI/INCITS RBAC Standard – Role Based Administration of RBAC: Crampton-Loizou Administrative model-Role control center								CO3	
UNIT IV	Role Engineering					Periods:9			
Scenario-driven role-engineering approach-Goal driven/hybrid role engineering approach - Tools for role discovery and role management - Role engineering: health care example-Enterprise Access Control Frameworks Using RBAC and XML Technologies								CO4	
UNITV	Integrating RBAC with Enterprise IT Infrastructures					Periods:9			
RBAC for WFMSs-RBAC integration in Web environments-RBAC for UNIX environments -RBAC in Java-RBAC for FDBSs-RBAC Features in Commercial Products.								CO5	

Lecture Periods: 45	Tutorial Periods:-	Practical Periods:-	Total Periods:45
<u>Reference Books</u>			
1. David F. Ferraiolo, D. Richard Kuhn, Ramaswamy Chandramouli, Role Based Access Control, Second Edition, Artech House, 2007. 2. Messaoud Benantar, Access Control Systems: Security, Identity Management and Trust Models, Springer, 2006.			

CO – PO Mapping

	PO1	PO2	PO3	PO4	PO5
CO1	2	2	3	-	-
CO2	3	1	3	-	-
CO3	3	3	3	-	2
CO4	3	3	3	2	1
CO5	3	3	3	2	-
Avg	2.8	2.4	3	2	1.5

Score: 3 – High; 2 – Medium; 1 – Low

Department: Computer Science and Engineering				Programme: M.Tech. (Information Security)					
Semester: I				Course Category Code: PSE			Semester Exam Type: TY		
Course Code	Course Name		Periods / Week			Credit	Maximum Marks		
			L	T	P			CA	SE
CSZ16	Secure Coding		3	-	-	3	40	60	100
Prerequisite	Nil								
Course Outcome	CO1	List the challenges and threats to building secure software systems.						Remember	
	CO2	Classify common validation errors, Buffer overflows and methods of managing exceptions						Understand	
	CO3	Identify possible security programming errors when conducting code reviews in languages such as Java, C or Python .						Apply	
	CO4	Identify the causes of security vulnerabilities in Web Applications						Apply	
	CO5	Identify privacy concerns in different contexts.						Apply	
UNIT I	Introduction					Periods : 9			
The Software Security Problem-Defensive Programming Is Not Enough-Security Features-The Quality Fallacy-Static Analysis in the Big Picture-Classifying Vulnerabilities-Introduction to Static Analysis-Problem Solving with static analysis-Type Checking - Style Checking- Program Understanding- verifications and property checking- Bug finding and Security Review								CO1	
UNIT II	Static Analysis					Periods : 9			
Performing a Code Review -Adding Security Review to an Existing Development Process - Static Analysis Metrics- Static Analysis Internals- Building a Model - Analysis Algorithms –Rules - Reporting Results								CO2	
UNIT III	Pervasive Problems					Periods : 9			
Handling Input - What to Validate - How to Validate - Preventing Metacharacter Vulnerabilities - Buffer Overflow – Strings – Integers - Runtime Protection - Errors and Exceptions - Handling Errors with Return Codes - Managing Exceptions - Preventing Resource Leaks - Logging and Debugging								CO3, CO1	
UNIT IV	Web Applications					Periods : 9			
Input and Output Validation for the Web - HTTP Considerations - Maintaining Session State - Using the Struts Framework for Input Validation								CO4, CO1	
UNIT V	Privacy and Privilege					Periods : 9			
Privacy and Regulation - Outbound Passwords - Random Numbers – Cryptography - Secrets in Memory - Implications of Privilege - Managing Privilege - Privilege Escalation Attacks								CO5	
Lecture Periods: 45		Tutorial Periods: -		Practical Periods: -		Total Periods: 45			

CO – PO Mapping

	PO1	PO2	PO3	PO4	PO5
CO1	-	-	1	-	-
CO2	-	-	1	-	2
CO3	2	1	1	-	2
CO4	2	1	1	-	2
CO5	-	1	1	-	3
Avg	2	1	1	-	2.2

Score: 3 – High; 2 – Medium; 1 – Low

Department: Computer Science and Engineering				Programme: M.Tech. (Information Security)					
Semester: I				Course Category Code: PSE			Semester Exam Type: TY		
Course Code CSZ17	Course Name Malware Analysis and Reverse Engineering		Periods / Week			Credit		Maximum Marks	
			L	T	P		CA	SE	TM
			3	-	-	3	40	60	100
Prerequisite	<ul style="list-style-type: none">Basics of operating systems (especially windows)Basics of programming and debugging skillsBasics of networking protocols								
Course Outcomes	CO1	Identify the cyber security challenges raised from malicious software attack							Apply
	CO2	Analyze the security risks, threats and potential vulnerabilities on enterprise networks environment.							Analyze
	CO3	Evaluate independent analysis of modern malware samples using behavioral, code analysis and memory forensic techniques							Evaluate
	CO4	Apply the learned techniques to protect, reduce the security risks and avoid malicious software attacks on computer systems or networks							Apply
	CO5	Develop research plan independently through learned skills and tools to investigate malicious software attacks and implement a cyber-protection plan							Apply
UNIT I							Periods : 9		
		Introduction: Fundamentals of Malware Analysis (MA),Basic Analysis: Basic Static Techniques, Malware Analysis in Virtual Machines, Basic Dynamic Analysis; Introduction to key MA tools and techniques, Behavioral Analysis vs. Code Analysis ;Understanding Malware Threats, Malware indicators, Malware Classification.							CO1, CO2
UNIT II							Periods : 9		
		Advanced Static Analysis: x86 Disassembly, IDA Pro, Recognizing C Code Constructs in Assembly Analysing Malicious Windows Programs Advanced Dynamic Analysis: Malware and Kernel Debugging - Opening and Attaching to Processes, Configuration of JIT Debugger for Shellcode Analysis, Controlling Program Execution, Setting and Catching Breakpoints, Debugging with Python Scripts and Py Commands, DLL Export Enumeration, Execution and Debugging, debugging a VMware Workstation Guest (on Windows)							CO2,CO3
UNIT III							Periods : 9		
		Malware Functionality: Malware Behavior, Covert Malware Launching, Data Encoding, Malware-Focused Network Signatures. Introduction to WinDbg Commands and Controls, Detecting Rootkits with WinDbg Scripts, Kernel Debugging with IDA Pro.							CO3,CO4
UNIT IV							Periods : 9		
		Introduction to Reverse Engineering, Extended Reverse Engineering using GDB							CO4, CO5

and IDA, Reverse Engineering Malware (REM) Methodology, Resources for Reverse-Engineering Malware (REM). Anti-Reverse-Engineering- Anti-Disassembly, Anti-Debugging, Anti-Virtual Machine Techniques, Packers and Unpacking				
UNIT V				Periods : 9
Analyses and Security Defenses, Symbolic execution and taint tracking, Runtime memory forensics ,Behavioral detection signatures ,Security hardening (ASLR, DEP, and CFI), case studies in malware detection and analysis				CO3, CO5
Lecture Periods: 45	Tutorial Periods: -	Practical Periods: -	Total Periods: 45	
<u>Reference Books</u>				
1.MichaelSikorski, Andrew Honig, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, William Pollock (2012). 2. Jamie Butler and Greg Hoglund, “Rootkits: Subverting the Windows Kernel”, Addison-Wesley, 2005. 3.Dang, Gazet, Bachaalany, “Practical Reverse Engineering”, Wiley, 2014. 4.Reverend Bill Blunden, “The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System” Second Edition, Jones & Bartlett, 2012.				

CO – PO Mapping

	PO1	PO2	PO3	PO4	PO5
CO1	2	2	3	2	2
CO2	2	1	3	2	1
CO3	2	1	2	2	1
CO4	2	1	3	2	2
CO5	2	2	2	2	2
Avg	2	1.4	2.6	2	1.6

Score: 3 – High; 2 – Medium; 1 – Low

Department: Computer Science and Engineering				Programme: M.Tech. (Information Security)					
Semester: I				Course Category Code: PSE			Semester Exam Type: TY		
Course Code	Course Name		Periods / Week			Credit	Maximum Marks		
			L	T	P			CA	SE
CSZ18	Machine Learning and Security		3	-	-	3	40	60	100
Prerequisite	Basic knowledge of statistics and familiarity with a programming language								
Course Outcomes	CO1	Apply the concept of Machine Learning in cyber security.						Apply	
	CO2	Implement the Machine Learning techniques in Network Attacks.						Apply	
	CO3	Apply the knowledge of Machine Learning in the real-world practical applications.						Apply	
	CO4	Demonstrate the security related Machine Learning tasks						Understand	
	CO5	Develop tools using Machine Learning.						Apply	
UNIT I	Introduction					Periods : 9			
Introduction to machine learning: Cyber Threat Landscape, The Cyber Attacker’s Economy, Definition of machine learning, real-world uses of machine learning in security, spam fighting: an iterative approach, limitations of machine learning in security Classifying and clustering: machine learning: problems and approaches, machine learning in practice: a worked example, training algorithms to learn, supervised classification algorithms, practical considerations in classification, clustering.								CO1, CO3	
UNIT II	Anomaly detection					Periods : 9			
when to use anomaly detection versus supervised learning, intrusion detection with heuristics, data-driven methods, feature engineering for anomaly detection, anomaly detection with data and algorithms, challenges of using machine learning in anomaly detection, response and mitigation, practical system design concerns.								CO1, CO2, CO3	
UNIT III	Malware analysis					Periods : 9			
Understanding malware-defining malware classification, Malware: Behind the scenes, Feature generation- data collection, generating features, feature selection, From features to classification								CO2, CO3	
UNIT IV	Network traffic analysis					Periods : 9			
Theory of network defense, machine learning and network security, building a predictive model to classify network attacks. Protecting the consumer web: monetizing the consumer web, Types of abuse and the data that can stop them, supervised learning for abuse problems, clustering abuse, and further directions in clustering.								CO2, CO3, CO4	
UNIT V	Production systems and Adversarial Machine Learning					Periods : 9			
Production systems: Defining machine learning system maturity and								CO4, CO5	

scalability, data quality, model quality, performance, maintainability, monitoring and alerting, Security and reliability, feedback and usability. Adversarial machine learning: Terminology, the importance of adversarial ml, security vulnerabilities in machine learning algorithms, attack technique: model poisoning, attack technique: evasion attack			
Lecture Periods: 45	Tutorial Periods: -	Practical Periods: -	Total Periods: 45
<u>Reference Books</u>			
1. Clarence Chio and David Freeman, Machine Learning and Security: Protecting Systems with Data and Algorithms, O'Reilly Media, Inc., 2018			
2. Kevin Murphy, Machine Learning: A Probabilistic Perspective, MIT Press, 2012.			
3. Trevor Hastie, Robert Tibshirani, Jerome Friedman, The Elements of Statistical Learning, Springer 2009.			
4. Christopher Bishop, Pattern Recognition and Machine Learning, Springer, 2007.			

CO – PO Mapping

	PO1	PO2	PO3	PO4	PO5
CO1	3	2	3	-	-
CO2	3	1	2	-	-
CO3	3	3	1	-	-
CO4	2	2	3	-	1
CO5	3	2	2	-	1
Avg	2.80	2	2.20	-	1

Score: 3 – High; 2 – Medium; 1 – Low

Department: Computer Science and Engineering				Programme: M.Tech. (Information Security)						
Semester: I				Course Category Code: PSE			Semester Exam Type: TY			
Course Code	Course Name			Periods / Week			Credit	Maximum Marks		
				L	T	P		CA	SE	TM
CSZ19	Secure and Resilient Software Development			3	-	-	3	40	60	100
Prerequisite		Nil								
Course Outcome		CO1	Describe security and resilience Principles in Agile and Scrum models.						Understand	
		CO2	Design secure software applications using best practices and standards.						Apply	
		CO3	Develop defensive software applications using secure coding.						Create	
		CO4	Apply tools for identifying security vulnerabilities in software systems.						Apply	
UNIT I		Introduction							Periods: 9	
Today's Software Development Practices - Over the Waterfall - Agile - Shift Left - Principles – Deconstructing Agile and Scrum: The Goals of Agile and Scrum - Agile/Scrum Terminology- Agile/Scrum Roles - Unwinding Sprint Loops - Development and Operations Teams – Secure and Resilient - Bad Design Led to Vulnerable Internet - HTTP Problems - Design Errors - Requirements & Design: The Keys to a Successful Software Project - Design Flaws - Solutions – Security and Resilience in the Software Development Life Cycle.									CO1, CO2	
UNIT II		Nonfunctional Requirements							Periods: 9	
System Quality Requirements Engineering (SQUARE) – Characteristics of Secure and Resilient Software: Functional versus Nonfunctional Requirements - Testing NFRs- Families of Nonfunctional Requirements - Characteristics of Good Requirements - Eliciting Nonfunctional Requirements - NFRs as Acceptance Criteria and Definition of Done – Security Requirements for Application Software - Security Control Types - Think Like an Attacker - Detailed Security Requirements.									CO2, CO3	
UNIT III		Secure Design Considerations							Periods: 9	
Security Perimeter - Attack Surface - Application Security and Resilience Principles - Mapping Best Practices to Nonfunctional Requirements — Design Phase Recommendations - Modeling Misuse Cases - Conduct Security Design and Architecture Reviews - Threat and Application Risk Modeling - Risk Analysis and Assessment - Rules of Thumb for Defect Removal or Mitigation - Needs for Information Assurance - Countering Threats through Proactive Controls - Architecture and Design Review Checklist.									CO2, CO4	
UNIT IV		Defensive Programming and Testing							Periods: 9	
The Evolution of Attacks - Threat and Vulnerability Taxonomies - Failure to Sanitize Inputs is the Scourge of Software Development - Input Validation and Handling -									CO3, CO4	

Attacks - Improper Input Handling - Validating Input Data - OWASP's Secure Coding Practices - Practices for Software Resilience and Secure Coding - Improve Software Security - Testing: Standardized Testing Policy - Security Test Cases - Static Code Analysis - Penetration Testing/Dynamic Analysis.			
UNIT V	DevOps and AppSec	Periods: 9	
Securing DevOps - Metrics and Maturity Models for Security and Resilience - OpenSAMM - Levels of Maturity - BSIMM – Frontiers for AppSec: Internet of Things - Blockchain - Web Application Firewalls - Machine Learning/Artificial Intelligence - Big Data.			CO2, CO4
Lecture Periods: 45	Tutorial Periods: -	Practical Periods: -	Total Periods: 45
Reference Books			
1. Mark S. Merkow, Secure, Resilient, and Agile Software Development, CRC Press, Taylor & Francis, 2019. 2. Mark S. Merkow and Lakshmikanth Raghavan, Secure and Resilient Software: Requirements, Test Cases, and Testing Methods, First Edition, CRC Press, Taylor & Francis, 2019. 3. Mark S. Merkow and Lakshmikanth Raghavan, Secure and Resilient Software Development, CRC Press, Taylor & Francis, 2010.			

CO – PO Articulation Matrix

	PO1	PO2	PO3	PO4	PO5
CO1	2	-	2	1	1
CO2	2	-	2	1	3
CO3	2	-	3	2	3
CO4	2	-	3	2	2
Avg	2	-	2.5	1.5	2.25

Score: 3 – High; 2 – Medium; 1 – Low

Department: Computer Science and Engineering			Programme: M.Tech.(Information Security)					
Semester: II			Course Category Code: PSE			Semester Exam Type: TY		
Course Code	Course Name	Periods / Week			Credit	Maximum Marks		
		L	T	P		CA	SE	TM
CSZ20	Data Mining and Knowledge Discovery	3	-	-	3	40	60	100
Prerequisite		Nil						
Course Outcome	CO1	Infer Data Preprocessing, Mining and Association Rules.					Understand	
	CO2	Infer the Classification, Prediction and Clustering techniques.					Understand	
	CO3	Understand the overall architecture of the data warehouse techniques					Understand	
	CO4	Make use of datamining tools and datawarehouse for developing business applications					Apply	
UNIT I	Data Mining, Preprocessing and Association					Periods : 9		
Data Mining: - Data Mining Functionalities – Data Mining Task, Integration of Data Mining System with a Database – Major issues in Data Mining. Data Preprocessing: Data Cleaning – Data Integration and Transformation – Data Reduction – Data Discretization and Concept Hierarchy Generation. Association Rule Mining: - Efficient and Scalable Frequent Item set Mining Methods – Mining Various Kinds of Association Rules –Association Mining to Correlation Analysis – Constraint-Based Association Mining.							CO1	
UNIT II	Classification and Prediction					Periods : 9		
Classification : - Issues Regarding Classification and Prediction – Classification by Decision Tree Induction – Bayesian Classification – Rule Based Classification – Classification by Back propagation – Support Vector Machines – Associative Classification – Lazy Learners – Other Classification Methods . Prediction - Accuracy and Error Measures – Evaluating the Accuracy of a Classifier or Predictor – Ensemble Methods – Model Section.							CO2	
UNIT III	Cluster Analysis					Periods : 9		
Cluster Analysis definition - Types of data in Cluster Analysis - Categorization of Clustering Methods -Partitioning Methods -Hierarchical methods - Density based Methods - Grid based Methods – Model based Clustering Methods – Constraint-Based Cluster Analysis - Outlier Analysis.							CO2	
UNIT IV	Data Warehousing and Business Analysis					Periods : 9		
Data warehousing Components –Building a Data warehouse – Mapping the Data Warehouse to a Multiprocessor Architecture – DBMS Schemas for Decision Support – Data Extraction, Cleanup, and Transformation Tools –Metadata – reporting – Query tools and Applications – Online Analytical Processing (OLAP) – OLAP and Multidimensional Data Analysis.							CO3, CO4	

UNIT V	Case Studies	Periods : 9	
Mining Streams -Time Series - Sequence Data - Mining of Complex Data Objects - Spatial Databases - Multimedia Databases, Text Databases-World Wide Web- Applications and Trends in Data Mining. Case Studies: Data Mining Techniques for Optimizing Inventories for Electronic Commerce, Crime Data Mining, Retailing Bank Customer Attrition Analysis.			CO3, CO4
Lecture Periods: 45	Tutorial Periods: -	Practical Periods: -	Total Periods: 45
Reference Books			
1. Jiawei Han and Micheline Kamber , Data Mining Concepts and Techniques, Second Edition,Elsevier,Reprinted 2008. 2. Alex Berson and Stephen J. Smith,Data Warehousing, Data Mining & OLAP , Tata McGraw –Hill Edition,Tenth Reprint 2007. 3. G. K. Gupta ,Introduction to Data Mining with Case Studies , Easter Economy Edition, PrenticeHall of India,2006. 4. K.P. Soman, Shyam Diwakar and V. Ajay ,Insight into Data mining Theory and Practice , EasterEconomy Edition, Prentice Hall of India, 2006. 5. Margaret H. Dunham, Data Mining: Introductory and Advanced Topics, Pearson Education,2004. 6. Alex Berson and Stephen J. Smith, Data Warehousing, Data mining and OLAP , Tata McGraw-Hill, 2004 7. Pang-Ning Tan, Michael Steinbach and Vipin Kumar,Introduction to Data Mining, Pearson Education, 2016.			

CO – PO Mapping

	PO1	PO2	PO3	PO4	PO5
CO1	1	-	1	-	-
CO2	1	-	1	-	-
CO3	2	-	-	-	-
CO4	3	3	3	3	2
Avg	1.75	3	1.66	3	2

Score: 3 – High; 2 – Medium; 1 – Low

Department:Computer Science and Engineering			Programme:M.Tech.(InformationSecurity)					
Semester:II			Course Category Code:PCC			Semester Exam Type:TY		
Course Code	CourseName	Periods/Week			Credit	MaximumMarks		
		L	T	P			CA	SE
CSZ21	Digital Forensics	3	-	-	3	40	60	100
Prerequisite		Nil						
Course Outcome	CO1	Explain the Forensic science and Digital Forensic concepts						Remember
	CO2	Evaluate various digital forensic Operandi and motive behind cyber attacks						Evaluate
	CO3	Describe the cyber pieces of evidence, forensic cloning of evidence and their legal perspective.						Understand
	CO4	Apply various forensic tool to investigate the cybercrime and to Identify the digital pieces of evidence						Apply
	CO5	Analyze the Digital Evidence used to commit cyber offences						Analyze
UNIT I	Introduction and Understanding of the technical concepts of Forensics							Periods:9
Understanding of forensic science, digital forensic, The digital forensic process, Locard’s exchange principle, Scientific models. Basic computer organization, File system, Memory organization concept, Data storage concepts								CO1
UNIT II	Digital Forensics Process Model							Periods:9
Introduction to cybercrime scene, Documenting the scene and evidence, maintaining the chain of custody, forensic cloning of evidence, Live and dead system forensic, Hashing concepts to maintain the integrity of evidence, Report drafting.								CO2
UNIT III	Computer Operating system Artifacts							Periods:9
Finding deleted data, hibernating files, examining window registry, recycle bin operation, understanding of metadata, Restore points and shadow copies								CO3
UNIT IV	Legal aspects of digital forensics and digital Forensic tools							Periods:9
Understanding of legal aspects and their impact on digital forensics, Electronics discovery Quality assurance, Tool validation, Tool selection, Hardware and Software tools								CO4
UNIT V	Case Study							Periods:9
Understanding of Internet resources, Web browser, Email header forensic, social networking sites								CO5
Lecture Periods:45		Tutorial Periods:-		Practical Periods:-			Total Periods:45	

ReferenceBooks

1. The basics of digital Forensics (Latest Edition) – The primer for getting started in digital forensics by John Sammons – Elsevier Syngress Imprint
2. Cybersecurity – Understanding of cybercrimes, computer forensics and Legal perspectives by Nina Godbole and SunitBelapure – Wiley India Publication
3. Practical Digital Forensics – Richard Boddington [PACKT] Publication, Open source community

CO–PO Mapping

	PO1	PO2	PO3	PO4	PO5
CO1	2	1	2	-	-
CO2	2	1	2	2	1
CO3	3	1	2	2	1
CO4	3	2	3	3	1
CO5	2	2	2	2	-
Avg	2.4	1.4	2.2	2.22	1

Score:3–High;2–Medium;1–Low

Department: Computer Science and Engineering		Programme: M.Tech. (Information Security)						
Semester: II		Course Category Code: PSE				Semester Exam Type: TY		
Course Code	Course Name	Periods / Week			Credit	Maximum Marks		
		L	T	P		CA	SE	TM
CS222	Biometric Security	3	-	-	3	40	60	100
Prerequisite		Nil						
Course Outcome	CO1	List the various Biometric Functionalities.					Remember	
	CO2	Enumerate the fundamental theories and basic algorithms for fingerprint, face and iris modalities					Understand	
	CO3	Paraphrase the various aspects of Behavioral Biometrics					Remember	
	CO4	Identify the sociological and acceptance issues associated with the design and implementation of biometric systems.					Apply	
	CO5	Analyze existing theories, methods and interpretations in the field of biometrics					Analyze	
UNIT I	Introduction						Periods : 9	
Traditional authentication methods and technologies, Person Recognition – Biometric systems –Biometric functionalities: verification, identification – Biometric systems errors - The design cycle of biometric systems – Applications of Biometric systems – Security and privacy issues.							CO1	
UNIT II	Finger Print and Facial Recognition						Periods : 9	
Fingerprint: Introduction – Friction ridge pattern- finger print acquisition: sensing techniques, image quality – Feature Extraction – matching – indexing. Face recognition: Introduction –Image acquisition: 2D sensors, 3D sensors- Face detection- Feature extraction -matching.							CO2 CO4	
UNIT III	Iris and other Traits						Periods : 9	
Design of an IRIS recognition system-IRIS segmentation- normalization – encoding and matching- IRIS quality –performance evaluation, other traits- ear detection –ear recognition –gait feature extraction and matching – challenge, hand geometry – soft biometrics.							CO2 CO4	
UNIT IV	Behavioral Biometrics						Periods : 9	
Introduction –Features- classification of behavioral biometrics –properties of behavioral biometrics – signature –keystroke dynamics –voice- merits –demerits.							CO3 CO4	
UNIT V	Applications and Trends						Periods : 9	
Bio-metric system Application areas: surveillance applications- personal applications – design and deployment -user system interaction-operational processes – architecture –application development –design validation-disaster recovery plan-maintenance- privacy concerns.							CO5	
Lecture Periods: 45		Tutorial Periods: -		Practical Periods: -			Total Periods: 45	

CO – PO Mapping

	PO1	PO2	PO3	PO4	PO5
CO1	-	-	1	-	-
CO2		-	1	-	-
CO3	-	-	1	-	-
CO4	-	-	-	2	3
CO5	1	3	-	1	-
Avg	1	3	1	1.5	3

Score: 3 – High; 2 – Medium; 1 – Low

Department: Computer Science and Engineering				Programme: M.Tech. (Information Security)					
Semester: II				Course Category Code: PSE			Semester Exam Type: TY		
Course Code	Course Name		Periods / Week			Credit	Maximum Marks		
			L	T	P		CA	SE	TM
CSZ23	Cyber Security Governance		3	-	-	3	40	60	100
Prerequisite	Nil								
Course Outcomes	CO1	Familiarize the security threat issues, cases and the management methodologies related to the real-world problems						Understand	
	CO2	Develop cyber security strategy, architectures and risk management process for security governance procedures						Apply	
	CO3	Formalize the governance’s policy in adopting standards for the organization						Apply	
	CO4	Identify the high-risk data to manage risks from external and internal threats						Apply	
UNIT I	Introduction, Managing Risk and Plan For Success						Periods : 9		
Introduction: Defining Cybersecurity, Cybersecurity is a Business Imperative, Cybersecurity is an Executive-Level Concern, Why Be Concerned? : A Classic Hack, Nation-State Threats, Cybercrime is Big Business. Managing Risk: Who Owns Risk in Your Business?, What are Your Risks? Calculating Your Risk, Communicating Risk, Organizing for Success. Build Your Strategy. Plan For Success :Turning Vision into Reality, Policies Complement Plans, Procedures Implement Plans, Exercise Your Plans, Legal Compliance Concerns, Auditing								CO1, CO2 ,CO4	
UNIT II	Change Management and Personnel Management						Periods : 9		
Change Management: Why Managing Change is Important, When to Change?, What is Impacted by Change?, Change Management and Internal Controls, Change Management as a Process, Best Practices in Change Management. Personnel Management: Finding the Right Fit, Creating the Team, Establishing Performance Standards, Organizational Considerations, Training for Success, and Special Considerations for Critical Infrastructure Protection. Performance Measures, What To Do When You Get Hacked: Hackers Already Have You Under Surveillance, Things to do Before its Too Late: Preparing for the Hack, What to do When Bad Things Happen, Foot Stompers								CO1,CO2	
UNIT III	Information Governance and Changing Technical, Corporate Landscape						Periods : 9		
The Case for Information Governance: Information Governance, The Small Business, The Medium Size Business, Large Business, What You will Learn. The Threats of Today and Tomorrow: Defining Threats, Future Concerns. The Ever Changing Technical Landscape: A Little History, The Issues, The World is Shrinking. The Changing Corporate Landscape: Today’s Cyber Environment, The Federal Government, The Private Sector, and Why Should Corporate America Care?								CO1,CO4	
UNIT IV	Information Governance Fits in the New World						Periods : 9		

How Information Governance Fits in the New World: Issues in the New World. The Human Element: Cyber, Physical Acts. The Technical Side: The Benefits, Concerns Brought About by Technology. Balancing Information Governance and Your Company's Mission: Policies, Factors to Consider			CO3
UNIT V	Information Governance from within Organization	Periods : 9	
The Case for Information Governance from within Your Organization: Negative Perceptions of Information Governance, Implementation. What to do First: The Basics, How to Determine Information Governance Needs for Your Company, How to Create Information Governance Policies, Methods of Security to Support Information Governance, How to Implement Information Governance Policies. What to do Forever: Continuing Efforts, Evaluate Effectiveness of Information Governance Policies, Encouraging Accountability and Ownership of Information Governance, Training and Education of Employees About Information Governance. Charting the Best Future Course for Your Organization: Information Governance Impacts All Facets of an Organization, Closing Thoughts			CO3
Lecture Periods: 45	Tutorial Periods: -	Practical Periods: -	Total Periods: 45
Reference Books			
<ol style="list-style-type: none"> 1. Touhill, G. & Touhil, C., Cybersecurity for Executives: A Practical Guide. Hoboken, NJ: John Wiley & Sons Inc, 2014 2. Iannarelli, J. G., & O'Shaughnessy, M. O, Information Governance and Security: Protecting and Managing Your Company's Proprietary Information. Waltham, MA: Butterworth Heinemann, Elsevier, 2015. 3. Bosworth, S., & Kabay, M.E., & Whyne, E., Computer Security Handbook, John Wiley & Sons Inc, 2014. 			

CO – PO Mapping

	PO1	PO2	PO3	PO4	PO5
CO1	1	-	2	1	-
CO2	2	1	1	2	1
CO3	1	1	1	1	1
CO4	2	2	1	1	2
Avg	1.5	1.3	1.25	1.25	1.3

Score: 3 – High; 2 – Medium; 1 – Low

Department: Computer Science and Engineering			Programme: M.Tech.(InformationSecurity)					
Semester: II			Course Category Code: PSE			Semester Exam Type: TY		
Course Code	Course Name	Periods / Week			Credit	Maximum Marks		
		L	T	P		CA	SE	TM
CS224	Cyber Physical Systems	3	-	-	3	40	60	100
Prerequisite	Nil							
Course Outcome	CO1	Learn the concept and application of cyber physical system					Understand	
	CO2	Understand the safety requirements of cyber physical system					Understand	
	CO3	Understand the liveness requirements of cyber physical system					Understand	
	CO4	Understand and design of dynamical system					Understand	
	CO5	Learn to design a system for timed process					Understand	
UNIT I	Introduction					Periods : 9		
Cyber-Physical System- Key Features of Cyber-Physical Systems -cyber components and physical components - Sensors and Actuators. Applications of Cyber Physicalsystems.							CO1	
UNIT II	Synchronous Model and Safety Requirements					Periods : 9		
Synchronous Model - Reactive Components - Variables, Valuations, and Expressions - Inputs, Outputs, and States- Initialization-Update - Executions - Extended-State Machines- Properties of Components. Finite-State Components-Combinational Components-Event-Triggered Components-Nondeterministic Components -Input-Enabled Components -Task Graphs and Await Dependencies. -Composing Components-Block Diagrams-Input/Output Variable Renaming -Parallel Composition- Output Hiding-Synchronous Designs -Synchronous Circuits- Cruise Control System- Synchronous Networks. Safety Requirements- Safety Specifications -Invariants of Transition Systems- Role of Requirements in System Design -Safety Monitors-VerifyingInvariants -Proving Invariants- Automated Invariant Verification- Simulation-Based Analysis - Enumerative Search-Symbolic Search-Symbolic Transition Systems-Symbolic Breadth-First Search - Reduced Ordered Binary Decision Diagrams.							CO2	
UNIT III	Asynchronous Model and Liveness Requirements					Periods : 9		
Asynchronous Model -Asynchronous Processes -States, Inputs, and Outputs - -Input, Output, and Internal Actions -Executions -Extended-State Machines -Operations on Processes -Safety Requirements -Asynchronous Design Primitives -Blocking vs. Non-blocking Synchronization-Deadlocks -Shared Memory -Fairness Assumptions*-Asynchronous Coordination- Protocols-Leader Election -Reliable Transmission-Wait-Free Consensus. Liveness Requirements: Temporal Logic-Linear Temporal Logic – Ltl Specifications- . Ltl Specifications for Asynchronous Processes-Beyond Ltl - Model Checking-Bu`chiAutomata -From Ltl to Buchi Automata- Nested Depth-First Search- Symbolic Repeatability Checking-Proving Liveness-Eventuality Properties Conditional Response Properties .							CO3	

UNIT IV	Dynamical Systems	Periods : 9	
Dynamical Systems -Continuous-Time Models - Continuously Evolving Inputs and Outputs -Models with Disturbance-Composing Components - Stability -Linear Systems -Linearity -Solutions of Linear Differential Equations .- Stability - Designing Controllers - Open-Loop vs. Feedback Controller-Stabilizing Controller -PID Controllers- AnalysisTechniques- Numerical Simulation - Barrier Certificates .			CO4
UNIT V	Timed Model	Periods : 9	
Timed Processes -Timing-Based Light Switch- Buffer with a Bounded Delay -Multiple Clocks-Formal Model- Timed Process Composition - Modeling Imperfect Clocks- Timing-Based Protocols -Timing-Based Distributed Coordination- Audio Control Protocol-Dual Chamber Implantable Pacemaker -Timed Automata - Model of Timed Automata -Region Equivalence-Matrix-Based Representation for Symbolic Analysis. Real-Time Scheduling: Scheduling Concepts -Scheduler Architecture -Periodic Job Model - Schedulability.-Alternative Job Models -EDF Scheduling- EDF for Periodic Job Model--Optimality of EDF.			CO5
Lecture Periods: 45	Tutorial Periods: -	Practical Periods: -	Total Periods: 45
Reference Books			
1. Lee, Edward Ashford, and SanjitArunkumarSeshia. Introduction to embedded systems: Acyber physicalsystems approach. Lee &Seshia, 2011. 2. Alur, Rajeev. Principles of Cyber-Physical Systems. MIT Press, 2015. 3. Wolf, Marilyn. High-Performance Embedded Computing: Applications in Cyber-PhysicalSystems andMobile Computing. Elsevier, 2014.			

CO – PO Mapping

	PO1	PO2	PO3	PO4	PO5
CO1	1	-	1	-	-
CO2	2	-	2	2	-
CO3	3	-	2	2	1
CO4	3	3	3	3	1
CO5	3	3	3	3	1
Avg	2.4	3	2.2	2.2	1

Score: 3 – High; 2 – Medium; 1 – Low

Department: Computer Science and Engineering				Programme: M.Tech. (Information Security)						
Semester: II				Course Category Code: PSE			Semester Exam Type: TY			
Course Code	Course Name		Periods / Week			Credit	Maximum Marks			
			L	T	P			CA	SE	TM
CSZ25	Intrusion Detection Systems		3	-	-	3	40	60	100	
Prerequisite		Nil								
Course Outcome	CO1	Identify suitable methods and processes for intrusion detection and prevention.						Apply		
	CO2	Evaluate malicious activity or policy violations in specific application domain.						Evaluate		
	CO3	Design network or host-based Intrusion Detection System for an organization.						Apply		
	CO4	Analyse intrusion detection alerts and logs to distinguish attack types from false alarms						Analyse		
	CO5	Apply Intrusion Detection tools to improve the security posture.						Apply		
UNIT I							Periods: 9			
The state of threats against computers, and networked systems-Overview of computer security solutions and why they fail-Vulnerability assessment, firewalls, VPN's -Overview of Intrusion Detection and Intrusion Prevention- Network and Host-based IDS.									CO1	
UNIT II							Periods: 9			
A General IDS model and taxonomy, Signature-based Solutions, Anomaly Detection Systems and Algorithms-Network Behavior Based Anomaly Detectors (rate based)- Host-based Anomaly Detectors-Software Vulnerabilities- State transition, Immunology, Payload Anomaly Detection.									CO1, CO3	
UNIT III							Periods: 9			
Types of exploits: Memory buffer overflow, format string overflow, polymorphic shell code, Worms and Botnets- Matching methods for detection of exploits: signature, rule, profile based -Attack trees and Correlation of alerts.									CO2, CO4	
UNIT IV							Periods: 9			
Email/IM security issues-Viruses/Spam-From signatures to thumbprints to zero-day detection-Insider Threat issues - Taxonomy-Masquerade and Impersonation-Traitors, Decoys and Deception, Collaborative Security.									CO2, CO4	
UNIT V							Periods: 9			
Snort IDS, modes of operation, components, rules, and output. Application domains: Critical Infrastructure, Fraud Detection, Medical and public health and wireless sensor Networks.									CO2, CO5	
Lecture Periods: 45		Tutorial Periods: -		Practical Periods: -		Total Periods: 45				
Reference Books										
1. Peter Szor, The Art of Computer Virus Research and Defense, Symantec Press, 2005.										

2. Markus Jakobsson and Zulfikar Ramzan, Crimeware, Understanding New Attacks and Defenses, Symantec Press, 2008.
3. Carl Endorf, Eugene Schultz and Jim Mellander, Intrusion Detection and Prevention, McGraw Hill, 2004.
4. Pathan, Al-Sakib Khan, The State of the Art in Intrusion Detection and Prevention, CRC Press, Taylor and Francis Group, Aurbach Publications, 2014.

CO – PO Mapping

	PO1	PO2	PO3	PO4	PO5
CO1	-	-	2	-	1
CO2	2	-	2	1	1
CO3	1	1	2	1	2
CO4	2	1	2	1	2
CO5	3	-	2	1	2
Avg	2	1	2	1	1.6

Score: 3 – High; 2 – Medium; 1 – Low

Department: Computer Science and Engineering						Programme: M.Tech.(Information Security)		
Semester: III		Course Category Code: PSE				Semester Exam Tpe: TY		
Course Code	Course Name	Periods / Week			Credit	Maximum Marks		
		L	T	P			CA	SE
CSZ26	Security in IoT	3	-	-	3	40	60	100
Prerequisite		Nil						
Course Outcome	CO1	Outline the security principles and methodologies for Internet of Things					Remember	
	CO2	Discuss the Security requirements and cryptographic fundamentals in Connected cars.					Remember	
	CO3	Investigate the privacy preservation and trust models for Healthcare					Understand	
	CO4	Design the cloud security architecture for internet of things.					Apply	
UNIT I	INTRODUCTION : SECURING THE INTERNET OF THINGS						Periods : 9	
Security Requirements in IoT Architecture - Security in Enabling Technologies - Security Concerns in IoT Applications. Security Architecture in the Internet of Things - Security Requirements in IoT - Insufficient Authentication/Authorization - Insecure Access Control - Threats to Access Control, Privacy, and Availability - Attacks Specific to IoT. Vulnerabilities – Secrecy and Secret-Key Capacity – Authentication/ Authorization for Smart Devices - Transport Encryption – Attack & Fault trees.							CO1	
UNIT II	CRYPTOGRAPHIC FUNDAMENTALS FOR IOT						Periods : 9	
Cryptographic primitives and its role in IoT – Encryption and Decryption – Hashes – Digital Signatures – Random number generation – Cipher suites – key management fundamentals – cryptographic controls built into IoT messaging and communication protocols – IoT Node Authentication.							CO2	
UNIT III	IDENTITY & ACCESS MANAGEMENT SOLUTIONS FOR IOT						Periods : 9	
Identity lifecycle – authentication credentials – IoT IAM infrastructure – Authorization with Publish / Subscribe schemes – access control							CO2	
UNIT IV	PRIVACY PRESERVATION AND TRUST MODELS FOR IOT						Periods : 9	

Concerns in data dissemination – Lightweight and robust schemes for Privacy protection – Trust and Trust models for IoT – self-organizing Things - Preventing unauthorized access.			CO3
UNIT V	CLOUD SECURITY FOR IOT		Periods : 9
Cloud services and IoT – offerings related to IoT from cloud service providers – Cloud IoT security controls – An enterprise IoT cloud security architecture – New directions in cloud enabled IoT computing.			CO4
Lecture Periods: 45	Tutorial Periods: -	Practical Periods: -	Total Periods: 45
<u>Reference Books</u>			
1. Brian Russell, Drew Van Duren, Practical Internet of Things Security, Packt Publishing, 2016. 2. Shancang Li Li Da XuImprint, Securing the Internet of Things, 2nd Edition, Syngress Publishers, Elsevier, 2017 3. Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations, CRC Press, 2016.			

CO – PO Mapping

	PO1	PO2	PO3	PO4	PO5
CO1	2	1	3	1	1
CO2	2	1	2	-	-
CO3	3	-	2	2	-
CO4	3	-	3	2	1
Avg	2.5	1	2.5	1.66	1

Score: 3 – High; 2 – Medium; 1 – Low

Department: Computer Science and Engineering					Programme: M.Tech.(Information Security)			
Semester: III		Course Category Code: PSE			Semester Exam Type: TY			
Course Code	Course Name	Periods / Week			Credit	Maximum Marks		
		L	T	P			CA	SE
CSZ27	Security in Cloud Computing	3	-	-	3	40	60	100
Prerequisite	Nil							
Course Outcome	CO1	Explore the concepts of cloud computing security and its related techniques					Understand	
	CO2	Examine the Virtualization techniques and Administrative VM Vulnerabilities in Linux					Analyse	
	CO3	Investigate the software Security and Cloud security Challenges in AWS (Amazon Web Services)					Analyse	
	CO4	Design the Security provision for Zoom software development					Apply	
UNIT I	Security Concepts					Periods: 9		
Confidentiality – privacy – integrity – authentication – non-repudiation – availability – access control – defence in depth – least privilege – application in cloud – Security importance in PaaS, IaaS and SaaS – Cryptographic Systems- Symmetric cryptography – stream ciphers – block ciphers – modes of operation – public-key cryptography – hashing – digital signatures – public-key infrastructures – key management – X.509 certificates – OpenSSL							CO1	
UNIT II	Multi-Tenancy Issues					Periods: 9		
Isolation of users/VMs – Virtualization System Security Issues- ESX and ESXi Security – ESX file system security – storage considerations – backup and recovery – Virtualization System Vulnerabilities- Management console vulnerabilities – management server vulnerabilities – administrative VM vulnerabilities – guest VM vulnerabilities – hypervisor vulnerabilities – hypervisor escape vulnerabilities – configuration issues – malware.							CO2	
UNIT III	Cloud software security and Risk issues					Periods: 9		

Cloud information security objectives –Cloud security services-security design principles-Secure cloud software requirements-Secure cloud software testing-Cloud computing and Business continuity planning/disaster recovery-The CIA Triad-Privacy and Compliance Risk-Threats to Infrastructure, Data and Access Control-Cloud service provider Risks			CO3
UNIT IV	Cloud Security Challenges and Security Architecture		Periods: 9
Security Policy Implementation-policy types-Computer Security Incident Response Team (CSIRT)- Virtualization Management-Virtual Threats-VM Security Recommendation-VM specific Security Techniques-Architectural Consideration General Issues-Trusted Cloud Computing-Secure Execution Environment and Communication-Microarchitecture-Identity Management and Access Control Autonomic Security			CO3
UNIT V	Cloud Computing life cycle Issues and Design		Periods: 9
Standards-The Distributed Management Task Force (DMTF)-International Organization for standardization (ISO)-Open Grid Forum (OGF)-Layered Security and IDS-Computer Security and Incident Response Time-Encryption and Key management-VM Life Cycle- Design Security of a Web Services Metering Interface – security provision for Business Model Scenarios – Security implementation of Virtual Services for Organizations-Application Monitoring Implementation			CO4
Lecture Periods: 45	Tutorial Periods: -	Practical Periods: -	Total Periods: 45
Reference Books			
1. Tim Mather, SubraKumaraswamy, ShahedLatif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Media, 1 edition, 2014. 2. Ronald L. Krutz, Russell Dean Vines, Cloud Security, 2016. John W. Rittinghouse and James F. Ransome, Cloud Computing Implementation, Management and Security 2015.			

CO – PO Mapping

	PO1	PO2	PO3	PO4	PO5
CO1	1	-	3	1	-
CO2	1	-	2	1	-
CO3	3	-	2	3	1
CO4	3	2	3	3	1
Avg	2	2	2.5	2	1

Score: 3 – High; 2 – Medium; 1 – Low

Department: Computer Science and Engineering				Programme: M.Tech.(Information Security)					
Semester: IV				Course Category Code: PSE			Semester Exam Type: TY		
Course Code	Course Name	Periods / Week			Credit	Maximum Marks			
		L	T	P		CA	SE	TM	
CSZ03	Artificial Intelligence and Intelligent Systems	3	-	-	3	40	60	100	
Prerequisite	Nil								
Course Outcome	CO1	Analyze the different search techniques to solve real world problems for which solutions are difficult to express using the traditional algorithmic approaches.					Analyze		
	CO2	Develop knowledge representation and reasoning systems that demonstrate intelligent behavior.					Apply		
	CO3	Design intelligent computing models to solve real world problems and evaluate them.					Apply		
	CO4	Implement new hybrid algorithms and validate their results.					Create		
UNIT I	Introduction and Search Techniques					Periods : 9			
History of AI, Problem-solving through search, state-space, blind search techniques: BFS, DFS, UCS, Heuristic search techniques - Best-first search, Greedy search, A* search, AO* search, Adversarial search: Mini-max search, alpha-beta cut off, Problem reduction – AND/OR Graphs, Constraint satisfaction problem, Means Ends Analysis.							CO1		
UNIT II	Knowledge Representation Techniques and Reasoning under uncertainty					Periods : 9			
Approaches for knowledge representation, Propositional Logic, Predicate Logic, Rule based knowledge representation, Conflict Resolution, Semantic networks, Forward Chaining, Backward Chaining, Unification an, Resolution, Managing Uncertainty– Probability Theory, Bayes Rule, Bayesian Belief Networks.							CO2		
UNIT III	Planning and Learning					Periods : 9			
State space planning, partial order planning, Planning graphs, Planning under uncertainty, Learning Types- Rote Learning, Learning by taking advice, Explanation based learning, Supervised and Unsupervised learning, Decision trees based learning, Reinforcement Learning.							CO2		
UNIT IV	Intelligent Computing Models					Periods : 9			
Introduction to Intelligent Systems, Knowing when to use Intelligent Systems, Modes of intelligent interaction, Artificial Neural Networks- Types, Activation functions, Learning algorithms, Fuzzy Logic- Fuzzy sets and operations, Fuzzy Rules, Fuzzy Inference, Evolutionary Algorithms- Genetic Algorithm, Swarm intelligence- Particle Swarm Optimization Algorithm.							CO3		
UNIT V	Hybrid Intelligent Systems					Periods : 9			
Need for hybridization, Types of hybrid intelligent systems – Neuro-Fuzzy Systems, Evolutionary Fuzzy Systems, Evolutionary Neural Networks, Case studies on the applications of hybrid Intelligence techniques.							CO4		
Lecture Periods: 45		Tutorial Periods: -		Practical Periods: -		Total Periods: 45			
Reference Books									
1. Stuart J Russell, Peter Norvig, “Artificial Intelligence- A Modern Approach”, 4 th Edition, Pearson Education, 2020.									
2. Geoff Hulten, “Building Intelligent Systems - A Guide to Machine Learning Engineering”, Apress, 1 st edition, 2018.									

3. Crina Grosan and Ajith Abraham, "Intelligent Systems- A Modern Approach", Springer Intelligent Systems Reference Library Book 17, 2011.

CO – PO Mapping

	PO1	PO2	PO3	PO4	PO5
CO1	2	-	2	2	-
CO2	2	-	2	2	-
CO3	2	2	3	2	1
CO4	3	2	3	2	2
CO5	2.25	2.0	2.5	2.0	1.5

Score: 3 – High; 2 – Medium; 1 – Low