KONGU ENGINEERING COLLEGE
PERUNDURAI ERODE – 638 060
(Autonomous)

VISION

To be a centre of excellence for development and dissemination of knowledge in Applied Sciences, Technology, Engineering and Management for the Nation and beyond.

MISSION

We are committed to value based Education, Research and Consultancy in Engineering and Management and to bring out technically competent, ethically strong and quality professionals to keep our Nation ahead in the competitive knowledge intensive world.

QUALITY POLICY

We are committed to

- Provide value based quality education for developing the student as a competent and responsible citizen.
- Contribute to the nation and beyond through the state-of-the-art technology.
- Continuously improve our services.

DEPARTMENT OF INFORMATION TECHNOLOGY

VISION

To be a centre of excellence for development and dissemination of knowledge in Information Technology for the Nation and beyond.

MISSION

Department of Information Technology is committed to:

MS1: To transform the students into innovative, competent and high quality IT professionals to meet the growing global challenges.

MS2: To impart value-based IT education to the students and enrich their knowledge

MS3: To endeavour for continuous upgradation of technical expertise of students to cater to the needs of the society

MS4: To achieve an effective interaction with industry for mutual benefits

2018 REGULATIONS

PROGRAM EDUCATIONAL OBJECTIVES (PEOs)

Post Graduates of M.Tech Information Technology (Information Cyber Warfare) will

PEO1: Contribute effectively to serve the society through information security enabled solutions and products adhere to cyber security laws

PEO2: Articulate fundamental concepts of cyber security and research findings to train professionals or to educate engineering students

PEO3: Carry out research in the field of cyber security and contribute significant solutions to the safety and security of nation and society

MAPPING OF MISSION STATEMENTS (MS) WITH PEOs

MS\PEO	PEO1	PEO2	PEO3
MS1	3	-	3
MS2	-	3	3
MS3	-	2	3
MS4	3	1	3

1 – Slight, 2 – Moderate, 3 – Substantial, BT - Bloom's Taxonomy

PROGRAM OUTCOMES (POs)	
Information Technology(ICW) Post Graduates will be able to:	
PO1:	Carry out research /investigation and development work to solve real world problems in the field of cyber security
PO2:	Write and present a substantial technical report on their own research findings
PO3:	Identify the issues and solutions with adequate professional foundation in Information Security and cyber threats to contribute in research, academics and industry.
PO4:	Analyze complex cyber threats problems and to apply independent judgment for synthesizing information to make intellectual and/or creative advances for conducting research in information security
PO5:	Engage in lifelong learning for career development to adapt to change in technological needs of cyber world

MAPPING OF PEOs WITH POs

PEO\PO	PO1	PO2	PO3	PO4	PO5
PEO1	3	2	2	-	2
PEO2	-	3	2	3	2
PEO3	3	1	2	-	2

1 – Slight, 2 – Moderate, 3 – Substantial

CURRICULUM BREAKDOWN STRUCTURE UNDER REGULATION 2018

Curriculum Breakdown Structure(CBS)	Curriculum content (% of total number of credits of the program)	Total number of contact hours	Total number of credits
Program Core(PC)	47.2%	510	34
Program Electives(PE)	25%	270	18
Project(s)/Internships(PR)/Others	27.8%	600	20
		Total Credits	**72**

KEC R2018: SCHEDULING OF COURSES –M.Tech- Information Technology (Information and Cyber Warfare)

Semester	Theory/ Theory cum Practical / Practical						Internship & Projects	Special Courses	Credits
	1	2	3	4	5	6	7	8	
I	18MWT11 Mathematical Foundations of Information Security (HS-3-1-0-4)	18MSC11 Data Structures and analysis of Algorithms (PC-3-0-2-4)	18MWC11 Computer Networks and Management (PC-3-0-2-4)	18MWT12 Principles of Secure Coding (PC-3-0-0-3)	18MWT13 Cyber Security and Cyber Law (PC-3-1-0-4)	18MWT14 Secure Software Engineering (PC-3-0-0-3)			22
II	18MWT21 Forensics and Incident Response (PC-3-0-0-3)	18MWC21 Ethical Hacking (PC-3-0-2-4)	18MWC22 Network Security Essentials (PC-3-0-2-4)	Professional Elective – I (PE-3-0-0-3)	Professional Elective – II (PE-3-0-0-3)	Professional Elective – III (PE-3-0-0-3)	18MWP21 Mini Proiect (PR-0-0-4-2)		22
III	Professional Elective – IV (PE-3-0-0-3)	Professional Elective – V (PE-3-0-0-3)	Professional Elective – VI (PE-3-0-0-3)	18MIL31 Computing Laboratory (PR-0-0-2-1)			18MWP31 Project Work - Phase I (PR-0-0-12-6)		16
IV							18MWP41 Project Work - Phase II (PR-0-0-24-12)		12

Total Credits: 72

KONGU ENGINEERING COLLEGE, PERUNDURAI, ERODE – 638 060
(Autonomous)

M.Tech. DEGREE IN INFORMATION TECHNOLOGY

(Information and Cyber Warfare)

CURRICULUM

(For the candidates admitted from academic year 2018-19 onwards)

SEMESTER – I

Course Code	Course Title	Hours / Week			Credit	Maximum Marks			CBS
		L	T	P		CA	ESE	Total	
	Theory/Theory with Practical								
18MWT11	Mathematical Foundations of Information Security	3	1	0	4	50	50	100	PC
18MSC11	Data Structures and Analysis of Algorithms	3	0	2	4	50	50	100	PC
18MWC11	Computer Networks and Management	3	0	2	4	50	50	100	PC
18MWT12	Principles of Secure Coding	3	0	0	3	50	50	100	PC
18MWT13	Cyber Security and Cyber Law	3	1	0	4	50	50	100	PC
18MWT14	Secure Software Engineering	3	0	0	3	50	50	100	PC
	Total				**22**				

CA – Continuous Assessment, ESE – End Semester Examination, CBS – Curriculum Breakdown Structure

KONGU ENGINEERING COLLEGE, PERUNDURAI, ERODE – 638 060
(Autonomous)

M.Tech. DEGREE IN INFORMATION TECHNOLOGY

(Information and Cyber Warfare)

CURRICULUM
(For the candidates admitted from academic year 2018-19 onwards)

SEMESTER – II

Course Code	Course Title	Hours / Week			Credit	Maximum Marks			CBS
		L	T	P		CA	ESE	Total	
	Theory/Theory with Practical								
18MWT21	Forensics and Incident Response	3	0	0	3	50	50	100	PC
18MWC21	Ethical Hacking	3	0	2	4	50	50	100	PC
18MWC22	Network Security Essentials	3	0	2	4	50	50	100	PC
	Elective - I	3	0	0	3	50	50	100	PE
	Elective - II	3	0	0	3	50	50	100	PE
	Elective - III	3	0	0	3	50	50	100	PE
	Practical								
18MWP21	Mini Project	0	0	4	2	100	0	100	PR
	Total				**22**				

CA – Continuous Assessment, ESE – End Semester Examination, CBS – Curriculum Breakdown Structure

KONGU ENGINEERING COLLEGE, PERUNDURAI, ERODE – 638 060
(Autonomous)

M.Tech. DEGREE IN INFORMATION TECHNOLOGY

(Information and Cyber Warfare)

CURRICULUM

(For the candidates admitted from academic year 2018-19 onwards)

SEMESTER – III

Course Code	Course Title	Hours / Week			Credit	Maximum Marks			CBS
		L	**T**	**P**		**CA**	**ESE**	**Total**	
	Theory/Theory with Practical								
	Elective - IV	3	0	0	3	50	50	100	PE
	Elective - V	3	0	0	3	50	50	100	PE
	Elective - VI	3	0	0	3	50	50	100	PE
	Practical								
18MIL31	Computing Laboratory	0	0	2	1	100	0	100	PC
18MWP31	Project Work Phase I	0	0	12	6	50	50	100	PR
	Total				**16**				

CA – Continuous Assessment, ESE – End Semester Examination, CBS – Curriculum Breakdown Structure

KONGU ENGINEERING COLLEGE, PERUNDURAI, ERODE – 638 060
(Autonomous)

M.Tech. DEGREE IN INFORMATION TECHNOLOGY

(Information and Cyber Warfare)

CURRICULUM
(For the candidates admitted from academic year 2018-19 onwards)

SEMESTER – IV

Course Code	Course Title	Hours / Week			Credit	Maximum Marks			CBS
		L	T	P		CA	ESE	Total	
	Practical								
18MWP41	Project Work Phase II	0	0	24	12	50	50	100	PR
	Total				**12**				

CA – Continuous Assessment, ESE – End Semester Examination, CBS – Curriculum Breakdown Structure

Total Credits: 72

LIST OF PROFESSIONAL ELECTIVES						
Course Code	**Course Title**	**Hours/Week**			**Credit**	**CBS**
		L	**T**	**P**		
SEMESTER II						
18MSC21	Machine Learning Techniques	3	0	2	4	PE
18MSE07	Big Data Analytics	3	0	2	4	PE
18MIT21	Cloud Architecture and Security	3	0	0	3	PE
18MIE04	Mobile and Wireless Security	3	0	0	3	PE
18MWE01	Secured Network Protocols	3	0	0	3	PE
18MWE02	Information Theory and Coding	3	0	0	3	PE
18MWE03	Multimedia Compression Techniques	3	0	0	3	PE
18MWE04	Advanced Operating Systems Security	3	0	0	3	PE
18MWE05	Unix Internals	3	0	0	3	PE
SEMESTER III						
18MWE06	Intrusion Detection	3	0	0	3	PE
18MWE07	Steganography and Digital Watermarking	3	0	0	3	PE
18MWE08	Video Analytics	3	0	0	3	PE
18MWE09	Web Application Security	3	0	0	3	PE
18MWE10	Game Theory and its Applications	3	0	0	3	PE
18MWE11	Biometric Security	3	0	0	3	PE
18MWE12	Cyber Physical Systems	3	0	0	3	PE
18MWE13	Security Assessment and Risk Analysis	3	0	0	3	PE
18MWE14	Database Security and Access Control	3	0	0	3	PE
18MWE15	Public Key Infrastructure and Trust management	3	0	0	3	PE
18MWE16	Internet Protocol and Security	3	0	0	3	PE

18MWT11 MATHEMATICAL FOUNDATIONS OF INFORMATION SECURITY

L	T	P	Credit
3	1	0	4

Preamble	To familiarize the students with the fundamental theorems, group and subgroups properties, fundamental principles of cryptosystem, number theory and algebraic geometry and these concepts will help the students in their master project work
Prerequisites	Nil

UNIT – I **9**

Elementary Number Theory: O and Ω notations - Time estimates for doing arithmetic - Divisibility and the Euclidean algorithm - Linear Diophantine equations - Congruences: Definitions and properties - Linear congruences and Quadratic congruences - Residue classes - Euler’s phi function - Fermat’s Little Theorem - Chinese Remainder Theorem - Exponentiation and Discrete logarithm - Quadratic residues - Legendre symbol - Jacobi symbol - Algebraic structures: groups, rings, fields , GF(2^n) fields (Theorems without proof).

UNIT – II **9**

Simple Cryptosystems: Enciphering Matrices - Encryption Schemes - Symmetric and Asymmetric Cryptosystems - Substitution Cipher: Affine cipher - Vigenere Cipher - Modern Stream Ciphers: One time pad - LFSR - Block ciphers - Use of Block Ciphers - Hill Cipher - Transposition Cipher - Multiple Encryption - Secure Cryptosystem - Problems in Advanced Encryption Standard(AES) - Problems in Data Encryption Standard. (Theorems without proof)

UNIT – III **9**

Public Key Cryptosystems: The idea of public key cryptography - The Diffie-Hellman Key Agreement Protocol - RSA Cryptosystem - Rabin cryptosystem - ElGamal cryptosystem - Signature Algorithms: RSA signature - ElGamal signature - Schnorr Signature - Digital signature standard - Knapsack problem - Zero-Knowledge Protocols: Fiat Shamir protocol - Guillou Quisquater protocol - Hash and MAC algorithms: MD5 - SHA and HMAC (Theorems without proof)

UNIT – IV **9**

Prime Generation, Testing and Factoring: Generation: Mersenne Prime - Fermat Prime - Testing: Divisibility algorithm - Fermat test - Square root test - Miller Rabin test - Factorization: Trial division method - Fermat method - Pollard rho (γ) method - Continued fraction method - The quadratic sieve method. (Theorems without proof)

UNIT – V **9**

Number Theory and Algebraic Geometry: Elliptic curves - Basic facts - Elliptic curve cryptosystems - Elliptic curve primality test - Elliptic curve factorization - Lenstra’s ecc factorization - Elliptic curve confidentiality and signature.(Theorems without proof)

Lecture:45, Tutorial:15, Total: 60

REFERENCES:

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. Serge Vaudenay, “Classical Introduction to Cryptography - Applications for Communication Security”, Springer, 2006.
4. Victor Shoup, “A Computational Introduction to Number Theory and Algebra”, Cambridge University Press, 2005.
5. Manezes A., Van Oorschot P. and Vanstone S., “Hand Book of Applied Cryptography”, CRC Press, 1996.
6. Coutinho S.C., “The Mathematics of Ciphers - Number Theory and RSA Cryptography”, A.K. Peters, Natick, Massachusetts, 1998.

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped** **(Highest Level)**
CO1:	infer the concepts and results of number theory	Understanding (K2)
CO2:	solve number theory concepts into various security applications	Applying (K3)
CO3:	compare the difference between zero knowledge protocols with symmetric and asymmetric protocols	Applying (K3)
CO4:	illustrate various prime number generation used for designing security protocols and for its analysis	Understanding (K2)
CO5:	examine various algebraic structures for designing security algorithm	Analyzing (K4)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	3	2			
CO2	2	3			
CO3			2	2	
CO4	1			3	
CO5	1		2		3

1 – Slight, 2 – Moderate, 3 – Substantial, BT - Bloom’s Taxonomy

18MSE11 USER INTERFACE DESIGN

L	T	P	Credit
2	0	2	3

Preamble	UID deals with design of responsive web application using Full Stack Web Development – MEAN ie MongoDB, ExpressJS, AngularJS and NodeJS.
Prerequisites	HTML,CSS and Javascript

UNIT – I **9**

Introduction to NoSQL Database - MongoDB: What is NoSQL Database - Why to Use MongoDB - Difference between MongoDB & RDBMS - Download & Installation - Common Terms in MongoDB – Implementation of Basic CRUD Operations using MongoDB.

UNIT – II **9**

Introduction to Server-side JS Framework – Node.js: Introduction - What is Node JS – Architecture – Feature of Node JS - Installation and setup - Creating web servers with HTTP (Request and Response) – Event Handling - GET and POST implementation - Connect to NoSQL Database using Node JS – Implementation of CRUD operations.

UNIT – III **9**

Introduction to TypeScript: TypeScript : Introduction to TypeScript – Features of TypeScript – Installation setup – Variables – Datatypes – Enum – Array – Tuples – Functions – OOP concepts – Interfaces – Generics – Modules – Namespaces – Decorators – Compiler options – Project Configuration.

UNIT – IV **9**

Introduction to Client-side JS Framework – Basics of Angular: Introduction to Angular - Needs and Evolution – Features – Setup and Configuration – Components and Modules – Templates – Change Detection – Directives – Data Binding - Pipes – Nested Components.

UNIT – V **9**

Client-side JS Framework – Forms and Routing in Angular: Template Driven Forms - Model Driven Forms or Reactive Forms - Custom Validators - Dependency Injection - Services - RxJS Observables - HTTP - Routing.

List of Exercises / Experiments :

1. Implementation of Basic CRUD Operations using MongoDB
2. Create web server connection with HTTP Request and HTTP Response
3. Implementation of Event Handling using GET and POST Method
4. Establish Connection to NoSQL Database using NodeJS and implement CURD operations
5. Demonstrate Inheritance and Interfaces using Typescript
6. Design a web application using AngularJS

Lecture:45, Practical:15, Total: 60

REFERENCES / MANUALS / SOFTWARES:

1. Nathan Rozentals, “Mastering TypeScript”, 2nd Edition, Packt Publishing, 2017.
2. Nathan Murray, Ari Lerner, Felipe Coury, Carlos Taborda, “ng-book, The Complete Book on Angular 6”, Createspace Publisher, 2018.

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped (Highest Level)**
CO1:	create NoSQL Database CURD operations using MongoDB	Creating (K6)
CO2:	develop server side applications using Node JS	Creating (K6)
CO3:	make use of Type Script to build web application	Applying (K3)
CO4:	summarize Angular features and create component based web pages	Understanding (K2)
CO5:	design a Full Stack web application	Creating (K6)
CO6:	design RWD to perform CURD operations with MongoDB	Creating (K6), Precision (S3)
CO7:	create web server connection with HTTP request and HTTP response	Applying (K3), Precision (S3)
CO8:	develop full stack application using angular for the given use case	Creating (K6), Precision (S3)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	1				1
CO2	2				2
CO3	2		2		3
CO4	2		2		3
CO5	1		1		1
CO6	2		2		2
CO7	3		2		3
CO8	1		2		2

1 – Slight, 2 – Moderate,   3 – Substantial, BT - Bloom’s Taxonomy

18MWC11 COMPUTER NETWORKS AND MANAGEMENT

L	T	P	Credit
3	0	2	4

Preamble	Computer Networks and Management course is intended to provide the outline the basic concepts of computer networks and Illustrate the operations of network traffic, congestion, controlling and Queuing delay models, compare different mechanism for Quality of Service and Internet protocols and also describe the concept and architecture of Network Management, Showcase the different network management protocols like SNMP and RMON
Prerequisites	Nil

UNIT – I **9**

Introduction to Computer Networks : Introduction - Reliable Transmission via Redundancy - Reliable transmission by retransmission - Routing and addressing - Link Layer Protocols and Technologies - Quality of Service overview

UNIT – II **9**

Transmission Control Protocol (TCP) and Switching and Queuing Delay Models: Introduction to UDP and TCP - User Datagram Protocol (UDP) - TCP and Reliable Byte Stream Service - Congestion Control - Fairness - Recent TCP Versions -TCP Wireless Links - Packet Switching in Routers - Queuing Model - Networks of Queues

UNIT – III **9**

Mechanisms for Quality of Service and Internet Protocols: Queue Scheduling - Policing - Active Queue Management - MPLS - Internet Protocol Version (IPV6)- Routing Protocols-Address Translation Protocols-Domain Name System (DNS) - Network Management Protocols - Network Tools

UNIT – IV **9**

Network Management and SNMP: Network Management: Goals, Organization and Functions - Network Management Architecture and Organization - Network Management Perspective - NMS platform – Current Status and future of Network Management – SNMP V1 Network Management- Basic Foundation standards, Models and languages – Organization and information Models - Communication and functional Models – SNMP V2 – SNMP V3

UNIT – V **9**

RMON, Network Management Tools and Applications: Remote Monitoring – RMON SMI and MIB – RMON1-RMON2-ATM Remote Monitoring – A Case Study of Internet Traffic using RMON – Network Management Tools, Systems and Engineering –System utilities for Management – Network Statistics Measurement Systems – MIB Engineering – NMS Design – Network Management Applications

List of Exercises / Experiments :

1. Implementation of Error Detection / Error Correction Techniques
2. Implementation of Stop and Wait Protocol and Sliding Window Protocol.
3. Simulation of ARP /RARP protocols.
4. Applications using TCP Sockets like
   i. Echo client and echo server ii. Chat iii. File Transfer
5. Applications using TCP and UDP Sockets like
   i. DNS ii. SNMP iii. File Transfer
6. Examining Network Address Translation (NAT)
7. Configuring Static and Dynamic Routing

8. Configuring a Cisco Router as a DHCP Server
9. To create scenario and study the performance of network with CSMA / CA protocol and compare with CSMA/CD protocols.
10. Study of Network simulator (NS) and simulation of Congestion Control Algorithms using NS

Lecture:45, Practical:30, Total:75

REFERENCES:

1. Ivan Marsic, “Computer Networks Performance and Quality of Service”, 1st Edition, Rutgers University, New Brunswick, New Jersey, http://www.ece.rutgers.edu/marsic/books/CN/, 2013.
2. Mani Subramanian “Network Management: Principles and Practice”, 2nd Edition, Pearson Edition, ISBN-13: 978-8131734049, ISBN- 10: 8131734048, 2010.
3. Olivier Bonaventure**,** “Computer Networking: Principles, Protocols and Practice”, By Creative Commons Attribution (CC BY) ISBN: 978-1-365- 18583-0, 2011.
4. Larry Peterson and Bruce S Davis, “Computer Networks: A System Approach”, 5th Edition, Elsevier, 2014, ISBN-13: 978-0123850591, ISBN- 10: 0123850592, 2014.
5. Douglas E. Comer, “Internetworking with TCP/IP, Principles, Protocols and Architecture”, 6th Edition, PHI, ISBN-13: 978-0136085300, ISBN- 10: 013608530X, 2014.

SOFTWARES:

1. C / C++ / Java
2. Network Simulator like NS2/Glomosim/Cisco Packet Tracer

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped (Highest Level)**
CO1:	describe the network services, protocols and architectures	Understanding (K2)
CO2:	identify the different congestion control techniques	Understanding (K2)
CO3:	illustrate effective communication mechanisms using techniques like connection establishment, queuing theory, and recovery	Applying (K3)
CO4:	interpret the SNMP protocols, standard MIBs and RMON	Applying (K3)
CO5:	select appropriate network management tools to monitor a network	Analyzing (K4)
CO6:	implement and compare three major data link layer protocols and different client server applications using TCP and UDP	Applying (K3), Precision (S3)
CO7:	configure a DHCP server for allocation of IP address to participate in communication to make routing decision with help static and dynamic routes	Applying (K3), Precision (S3)
CO8:	make comparison between two widely used MAC protocols of data link layer	Analyzing (K4), Precision (S3)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	2	1	1	1	
CO2	1		2		1
CO3			2	1	
CO4			2	1	
CO5			1	2	1
CO6	3	2	1	1	
CO7	3	2	1	1	
CO8	3	2	1	1	

1 – Slight, 2 – Moderate, 3 – Substantial, BT - Bloom’s Taxonomy

18MWT12 PRINCIPLES OF SECURE CODING

L	T	P	Credit
3	0	0	3

Preamble	Commonly exploited software vulnerabilities are usually caused by avoidable software defects. Overcoming these defects during the process of development of software leads to secure coding practices. So, the purpose of this course is to identify, explain and demonstrate the problems in insecure coding practices and methods to rectify the same
Prerequisites	Programming languages

UNIT – I **9**

Contemporary Security: Need for secure systems - Proactive security development process - Security principles to live by and threat modeling

UNIT – II **9**

Secure Coding in C: Character strings - String manipulation errors - String Vulnerabilities and exploits - Mitigation strategies for strings - Pointers - Mitigation strategies in pointer based vulnerabilities - Buffer Overflow based vulnerabilities

UNIT – III **9**

Secure Coding in C++ and Java: Dynamic Memory Management - Common errors in dynamic memory management - Memory managers - Double -free vulnerabilities - Integer security - Mitigation strategies

UNIT – IV **9**

Database and Web Specific Input Issues: Quoting the Input - Use of stored procedures - Building SQL statements securely - XSS related attacks and remedies

UNIT – V **9**

Software Security Engineering: Requirements engineering for secure software: Misuse and abuse cases - SQUARE process model - Software security practices and knowledge for architecture and design

Total: 45

REFERENCES:

1. Michael Howard and David LeBlanc, “Writing Secure Code”, 2nd Edition, Microsoft Press.
2. Robert C. Seacord, “Secure Coding in C and C++”, 2nd Edition, Pearson Education.
3. Julia H. Allen, Sean J. Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead, “Software Security Engineering: A Guide for Project Managers”, Addison-Wesley Professional.

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped (Highest Level)**
CO1:	illustrate the need for secure coding and the importance of proactive development process	Applying (K3)
CO2:	examine the common security flaws in string manipulation and its resulting vulnerabilities	Analyzing (K4)
CO3:	identify the vulnerabilities in dynamic memory management	Analyzing (K4)
CO4:	critically analyze the input issues related to database and xss	Analyzing (K4)
CO5:	summarize the web fundamental principles of software security engineering	Understanding (K2)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	3		3		
CO2	2		2	2	
CO3	3		3		
CO4	3		3	2	
CO5	3		3		

1 – Slight, 2 – Moderate,   3 – Substantial, BT - Bloom’s Taxonomy

18MWT13 CYBER SECURITY AND CYBER LAW

L	T	P	Credit
3	1	0	4

Preamble	The objective of the course is to enrich the knowledge about cybercrime , cybercriminals and the areas affected by cybercrime and to investigate it
Prerequisites	Nil

UNIT – I 9

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

UNIT – II 9

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

UNIT – III 9

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

UNIT – IV 9

Understanding Computer Forensics: Understanding the Requirements - Computer Forensics and Steganography - Relevance of the OSI 7 - Layer Model to Computer Forensics - Forensics and Social Networking Sites: The Security/Privacy Threats - Computer Forensics from Compliance Perspective - Challenges in Computer Forensics - Special Tools and Techniques - Forensics - Auditing

UNIT – V 9

Introduction to Security Policies and Cyber Laws: Need for an Information-Security Policy- Information Security Standards - ISO - Introducing Various Security - Policies and their Review – Process - Introduction to Indian Cyber Law.

Lecture:45, Tutorial:15, Total: 60

REFERENCES:

1. Sunit Belapure and Nina Godbole, “Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives”, Wiley India Pvt. Ltd., ISBN: 978-81-265-21791, 2013.
2. Dr. Surya Prakash Tripathi, Ritendra Goyal, Praveen Kumar Shukla, KLSI., “Introduction to Information Security and Cyber Laws”, Dreamtech Press, ISBN: 9789351194736, 2015
3. Thomas J. Mowbray, “Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions”, John Wiley & Sons Inc., ISBN: 978 -1-118 - 84965 -1
4. James Graham, Ryan Olson, Rick Howard, “Cyber Security Essentials”, CRC Press, 2010.

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped (Highest Level)**
CO1:	summarize the area of cybercrime and forensics	Understanding (K2)
CO2:	examine the areas affected by cybercrime and investigation	Applying (K3)
CO3:	discriminate the Tools used in cyber forensic	Analyzing (K4)
CO4:	investigate the computer and identify the challenges associated with it	Analyzing (K4)
CO5:	outline the Legal preceptors in cyber security	Applying (K3)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1			3	1	
CO2	2	2	3	1	
CO3	2			2	
CO4	3		1	3	
CO5			3		1

1 – Slight, 2 – Moderate, 3 – Substantial, BT - Bloom’s Taxonomy

18MWT14 SECURE SOFTWARE ENGINEERING

L	T	P	Credit
3	0	0	3

Preamble	A software development perspective to the challenges of engineering software systems that is secure. This course addresses design and implementation issues critical to producing secure software systems.
Prerequisites	Software Engineering, UML, Data Structures, Java Programming

UNIT – I **9**

Problem, Process, and Product: Problems of software practitioners – Approach through software reliability engineering - Experience with SRE - SRE process - defining the product - Testing acquired software – reliability concepts- software and hardware reliability - Implementing Operational Profiles **-** Developing, identifying, crating, reviewing the operation – concurrence rate – occurrence probabilities - applying operation profiles

UNIT – II **9**

Engineering Reliability: Engineering “Just Right” Reliability **-** Defining “failure” for the product - Choosing a common measure for all associated systems - Setting system failure intensity objectives –Determining user needs for reliability and availability, overall reliability and availability objectives, common failure intensity objective, developed software failure intensity objectives – Engineering software reliability strategies - Preparing for Test - Preparing test cases - Planning number of new test cases for current release -Allocating new test cases - Distributing new test cases among new operations - Detailing test cases - Preparing test procedures

UNIT – III **9**

Executing Test: Planning and allocating test time for the current release - Invoking test identifying - identifying failures - Analyzing test output for deviations – Determining which deviations are failures - Establishing when failures occurred - Guiding Test - Tracking reliability growth - Estimating failure intensity - Using failure intensity patterns to guide test – Certifying reliability - Deploying SRE - Core material - Persuading your boss, your coworkers, and stakeholders - Executing the deployment - Using a consultant.

UNIT – IV **9**

Using UML for Security: UML diagrams for security requirement - security business process – physical security - security critical interaction - security state - Analyzing Model **-** Notation - formal semantics - security analysis - important security opportunities - Model based security engineering with UML - UML sec profile- Design principles for secure systems – Applying security patterns

UNIT – V **9**

Applications: Secure channel - Developing Secure Java program- more case studies - Tool support for UML Sec - Extending UML CASE TOOLS with analysis tools - Automated tools for UML SEC - Formal Foundations - UML machines - Rely guarantee specifications- reasoning about security properties

Total: 45

REFERENCES:

1. John Musa D., “Software Reliability Engineering”, 2nd Edition, Tata McGraw-Hill, 2005 (Units I, II and III)
2. Jan Jürjens, “Secure Systems Development with UML”, Springer; 2004 (Unit IV and V)

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped (Highest Level)**
CO1:	understand the terminology, the process and the models of the software reliability engineering	Understanding (K2)
CO2:	determine appropriate mechanisms for protecting the software system	Applying (K3)
CO3:	integrate requirements into secured software development process and test the software for security vulnerability	Applying (K3)
CO4:	examine secure design principles for developing attack resistant software	Analyzing (K4)
CO5:	evaluate a security solution for a given application, system with respect to security of the system	Evaluating (K5)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	2	1	2	2	3
CO2	3	2	3	3	3
CO3	3	1	3	3	3
CO4	3	1	2	3	2
CO5	3	2	3	3	3

1 – Slight, 2 – Moderate, 3 – Substantial, BT - Bloom’s Taxonomy

18MWT21 FORENSICS AND INCIDENT RESPONSE

L	T	P	Credit
3	0	0	3

Preamble	The course focuses on the procedures for identification, preservation, and extraction of electronic evidence, auditing and investigation of network and host system intrusions, analysis and documentation of information gathered, and preparation of expert testimonial evidence
Prerequisites	Nil

UNIT – I **9**

Incident and Incident Response : Introduction to Incident - Incident Response Methodology – Steps - Activities in Initial Response Phase after detection of an incident

UNIT – II **9**

Initial response and forensic duplication: Initial Response & Volatile Data Collection from Windows system - Initial Response & Volatile Data Collection from Unix system - Forensic Duplication: Forensic duplication: Forensic Duplicates as Admissible Evidence, Forensic Duplication Tool Requirements, Creating a Forensic Duplicate/Qualified Forensic Duplicate of a Hard Drive

UNIT – III **9**

Storage and Evidence Handling: File Systems-FAT,NTFS - Forensic Analysis of File Systems - Storage Fundamentals-Storage Layer, Hard Drives Evidence Handling-Types of Evidence, Challenges in evidence handling, Overview of evidence handling procedure

UNIT – IV **9**

Network Forensics : Collecting Network Based Evidence - Investigating Routers - Network Protocols - Email Tracing - Internet Fraud

UNIT – V **9**

Systems Investigation and Ethical Issues: Data Analysis Techniques - Investigating Live Systems (Windows & Unix) - Investigating Hacker Tools - Ethical Issues – Cyber crime

Total: 45

REFERENCES:

1. Kevin Mandia, Chris Prosise, “Incident Response and Computer Forensics”,Tata McGrawHill, 2nd Edition
2. Peter Stephenson, “Investigating Computer Crime: A Handbook for Corporate Investigations”
3. Eoghan Casey, "Handbook Computer Crime Investigation's Forensic Tools and Technology", Academic Press, 1st Edition, 2001.
4. Skoudis. E., Perlman. R. Counter Hack: “A Step-by-Step Guide to Computer Attacks and Effective Defenses”, .Prentice Hall Professional Technical Reference, 2001.
5. Norbert Zaenglein, “Disk Detective: Secret You Must Know to Recover Information From a Computer”, Paladin Press, 2000.

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped** **(Highest Level)**
CO1:	plan and prepare for all stages of an investigation detection and initial response	Applying (K3)
CO2:	describe the importance of evidence handling and storage	Understanding (K2)
CO3:	collect data from windows system and create a forensic duplicate of a hard disk	Applying (K3)
CO4:	monitor and collect evidence from network ,email and internet	Applying (K3)
CO5:	investigate live systems and aware of ehical issues	Applying (K3)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	3	1			
CO2	2	3	2		
CO3	3		3	1	
CO4	1	1	2		

1 – Slight, 2 – Moderate,   3 – Substantial, BT - Bloom’s Taxonomy

18MWC21 ETHICAL HACKING

(Common to Information Technology (Information Cyber Warfare) & Information Technology branches)

L	T	P	Credit
3	0	2	4

Preamble	This subject provides the fundamental knowledge about security permissions in computer, internet and system and how to secure from the various vulnerabilities and provide countermeasures for real world applications.
Prerequisites	Nil

UNIT – I **9**

Casing the Establishment: What is foot printing? - Internet Foot printing- Scanning – Determining if the system is alive – Determining which services are running or Listening – Detecting the operating system – Processing and storing scan data - Enumeration - basic banner grabbing- Enumerating Common Network services- Case study- Network Security Monitoring.

UNIT – II **9**

System Hacking: Introduction – Cracking password – Password cracking websites – Password guessing Algorithms – Password Cracking Tools – Countermeasure – Escalating Privileges- Executing Applications – Key loggers and spywares.

UNIT – III **9**

Infrastructure and Hardware Hacking: Remote connectivity and VoIP Hacking - Preparing to dial up-War – Dialing - Brute-Force Scripting - PBX hacking - Voice mail hacking - VPN hacking – Hacking Hardware – Physical access –Hacking Devices – Default Configurations – Reverse Engineering Hardware.

UNIT – IV **9**

Wireless and Firewall Hacking: Wireless Equipment – Discovery and monitoring - Denial of Service Attacks – Common Dos Attack Techniques - DoS Countermeasures - Encryption attacks –Authentication attacks - Firewalls - Firewalls landscape - Firewall Identification - Scanning Through firewalls - Packet Filtering - Application Proxy Vulnerabilities.

UNIT – V **9**

Application Hacking and Countermeasures : Web and Database Hacking – Web Server Hacking - Web application Hacking - Common web application Vulnerabilities – Database Hacking – Mobile Hacking – Hacking android – iOS.

List of Exercises / Experiments :

1. Passive Information Gathering
2. Detecting Live Systems
3. Enumerating Systems
4. Defeating Malware
5. Securing Wireless Systems - Net Stumbler
6. Capture Wireless Traffic
7. Breaking into Database using SQL Injection
8. OS Hacking
9. E-mail Bombing
10. Hacking android phone

Lecture: 45, Practical: 30, Total: 75

REFERENCES / MANUAL / SOFTWARES:	
1.	Stuart McClure, Joel Scambray and Goerge Kurtz, "Hacking Exposed 7 : Network Security Secrets and Solutions", 7th Edition, Tata McGrawHill Publishers, 2012.
2.	EC- Council Press, "Ethical Hacking and Countermeasures: Threats and Defense Mechanisms", 1st Edition, Cengage Learning, 2009.
3.	EC- Council Press, "Ethical Hacking and Countermeasures: Attack Phases", 1st Edition, Cengage Learning, 2009.

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped (Highest Level)**
CO1:	explain the basic vulnerabilities in any computing system	Applying (K3)
CO2:	determine the possible security attacks in complex real time systems and their effective countermeasures	Applying (K3)
CO3:	identify the security issues in hardware and software	Applying (K3)
CO4:	interpret the vulnerabilities in wireless environment and firewall systems	Applying (K3)
CO5:	formulate research problems in the computer security applications	Analyzing (K4)
CO6:	organize various information using passive information gathering, live system, enumeration and malware	Applying (K3), Precision (S3)
CO7:	utilize various tools to break the remote system hardware and software	Applying (K3), Precision (S3)
CO8:	examine various countermeasures for the vulnerabilities in real world applications	Analyzing (K4), Articulation (S4)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	3	2	3	3	2
CO2	3	2	3	3	2
CO3	3	2	3	3	2
CO4	3	2	3	3	2
CO5	3	3	3	3	3
CO6	3	2	3	3	2
CO7	3	2	3	3	2
CO8	3	3	3	3	3
1 – Slight, 2 – Moderate, 3 – Substantial, BT - Bloom's Taxonomy					

18MWC22 NETWORK SECURITY ESSENTIALS

(Common to Information Technology (Information Cyber Warfare), Communication Systems & Embedded Systems branches)

L	T	P	Credit
3	0	2	4

Preamble	To introduce the security problems associated with malicious software and intruders and familiarize the network security controls that help to protect the usability, integrity, reliability and safety of the network infrastructure and the data that travels through it.
Prerequisites	Computer Networks

UNIT – I **9**

Introduction: Characteristics of Networks, Need for network security, Intruders, Malicious Software, Reconnaissance, Eavesdropping, wiretapping, impersonation, traffic analysis, website defacement, DOS, active code or mobile code attacks, OSI Security Architecture, Security Services, Model for Network Security.

UNIT – II **9**

Cryptography and Key Distribution: Classical Encryption Techniques, Symmetric Encryption Principles, Symmetric Encryption Algorithms, DES, AES, Stream Ciphers, Block Cipher Modes of Operation, Public Key Cryptography Principles, Public Key Cryptographic Algorithms, RSA,ECC, Key Distribution using Symmetric and Asymmetric Encryption, Kerberos, X.509, Public Key Infrastructure, trust models, revocation, directories.

UNIT – III **9**

Message Authentication and Digital Signatures: Requirement of Authentication Functions, Message Authentication Codes, Hash and MAC Algorithms, MD2, MD4,MD5, SHA, HMAC, CMAC, Whirlpool, Address bases authentication, password based authentication, trusted intermediaries, digital Signatures, Digital Signature Standard.

UNIT – IV **9**

IP Security, Transport Layer Security: IP Sec, Authentication header, Encapsulating Security Payload, IKE, ISAKMP/IKE Encoding, Web Security Issues, Secure Sockets Layer, Transport Layer Security, Negotiating cipher suites, compression methods , encoding, HTTPS, Secure Shell.

UNIT – V **9**

Network Security Applications: Electronic Mail Security, Privacy enhanced mail, PGP, SMIME, Authorization and Access control, Firewalls, Intrusion Detection and Prevention Systems, Honeypots, honetnets, scanning and analysis tools, Antivirus Software, Virtual Private Network.

List of Exercises / Experiments :

1. Implement the following substitution and transposition techniques concepts
   a. Playfair Cipher
   b. Column Transformation
2. Implement Hill Cipher Technique
3. Implement the RSA Asymmetric key algorithm
4. Implement the Diffie Hellman Asymmetric key algorithm
5. Implement the Digital Signature standard algorithm
6. Setup a honey pot and monitor the honey pot on network (KF Sensor)
7. Demonstrate Intrusion Detection System (IDS) using any tool (snort or any other s/w)

Lecture: 45, Practical: 30, Total: 75

REFERENCES / MANUALS / SOFTWARES:	
1.	William Stallings, “Cryptography and Network Security Principles and Practices”, 6th Edition, Prentice Hall, 2013.
2.	Behrouz A. Fourouzan, “Cryptography and Network Security”, 2nd Edition, Tata McGraw-Hill, 2012.
3.	Charlie Kaufman, RadiaPeralman, Mike Speciner, “Network Security: Private communication in public world”, 2nd Edition, Prentice Hall, 2002.

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped (Highest Level)**
CO1:	identify the attacks against network infrastructure and the sources of attacks	Understanding (K2)
CO2:	evaluate the design principles of conventional encryption and public key encryption	Applying (K3)
CO3:	narrate the MAC and hashing techniques needed for authentication	Understanding (K2)
CO4:	identify the various types of security controls available to protect the network infrastructure	Understanding (K2)
CO5:	implement appropriate security controls to safeguard the network infrastructure	Applying (K3)
CO6:	practice the different types of symmetric key cryptographic algorithms	Applying (K3), Precision (S3)
CO7:	implement the various types asymmetric key cryptographic algorithms	Applying (K3), Precision (S3)
CO8:	demonstrate the different types of firewalls and intrusion detection system	Applying (K3), Precision (S3)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	3	1	3	2	2
CO2	2	1	2	2	1
CO3	2	1		1	
CO4	2	2	2	2	1
CO5	2	1	2	2	2
CO6	3	2	1	1	
CO7	2	2	1	1	
CO8	3	2	1	1	

1 – Slight, 2 – Moderate, 3 – Substantial, BT - Bloom’s Taxonomy

18MIL31 COMPUTING LABORATORY

(Common to Information Technology & Information Technology(Information Cyber Warfare) branches)

L	T	P	Credit
0	**0**	**2**	**1**

Preamble	This course aims to develop simple web applications in cloud, to design and development process involved in creating a cloud based application and to setup and configure web services and create web applications
Prerequisites	Web Technologies, Cloud Architecture

List of Experiments:

1. Install Virtual box/VMware Workstation with different operating systems.
2. Install and configure to launch virtual machine using trystack
3. Simulate a cloud scenario using CloudSim and implement a scheduling algorithm
4. Configure Google App Engine and create simple web applications using python/java.
5. Study experiment on configuring EC2 in Amazon Web Service
6. Design an online examination system using IaaS as service
7. Design an online book shopping cart system using server less computing

Total: 30

REFERENCES/MANUAL/SOFTWARES:

1.	Cloudsim, Trystack, Python/Java/PHP, HTML/Javascript/XAMPP, Virtualbox / VMWare, GoogleApp
2.	Laboratory Manual

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped (Highest Level)**
CO1:	configure various virtualization tools and simulate cloud environment and implement scheduling algorithms	Applying (K3), Precision (S3)
CO2:	configure various Web Services and launch virtual machine	Applying (K3), Precision (S3)
CO3:	develop and deploy web applications in cloud environment	Applying (K3), Precision (S3)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	1	2			
CO2			3		
CO3			3	3	2

1 – Slight, 2 – Moderate, 3 – Substantial

18MSC21 MACHINE LEARNING TECHNIQUES

(Common to Computer Science and Engineering, Information Technology, Information Technology (Information Cyber Warfare) & Control and Instrumentation Engineering branches)

L	T	P	Credit
3	0	2	4

Preamble	Provides a concise introduction to the fundamental concepts of machine learning and popular machine learning algorithms.
Prerequisites	Nil

UNIT – I **9**

Supervised Learning: Definition of Machine Learning - Examples of Machine Learning Applications. Supervised Learning:Learning a Class from Examples - VC Dimension - PAC Learning - Noise - Learning Multiple Classes - Regression - Model Selection and Generalization - Dimensions of a Supervised Machine Learning Algorithm. Dimensionality Reduction: Introduction - Subset Selection – Principal Component Analysis- Feature Embedding - Factor Analysis.

UNIT – II **9**

Tree And Probabilistic Models: Learning with Trees – Decision Trees – Constructing Decision Trees – Classification and Regression Trees – Different ways to Combine Classifiers – Boosting – Bagging — Gaussian Mixture Models – Nearest Neighbor Methods – Unsupervised Learning – K means Algorithm.

UNIT – III **9**

Multilayer Perceptrons: Introduction - The Perceptron - Training a Perceptron - Learning Boolean Functions - Multilayer Perceptrons - MLP as a Universal Approximator - Backpropagation Algorithm - Training Procedures - Tuning the Network Size - Dimensionality Reduction - Learning Time

UNIT – IV **9**

Kernel Machines: Introduction - Optimal Separating Hyperplane - Soft Margin Hyperplane - v-SVM - Kernal Trick - Vectorial Kernels - Defining Kernels - Multiple Kernel Learning - Multiclass Kernel Machines - One class Kernel Machines - Kernel Dimensionality Reduction.

UNIT – V **9**

Reinforcement Learning: Introduction - Single State Case-Elements of Reinforcement Learning - Model-Based Learning - Temporal Difference Learning - Generalization - Partially Observable States. Design of Machine Learning Experiments: Introduction - Factors, Response, and Strategy of Experimentation - Response Surface Design - Randomization, Replication, and Blocking - Guidelines for Machine Learning Experiments.

List of Exercises / Experiments :

1. Implementation of linear regression
2. Implementation of Decision tree
3. Implementation of k-means clustering
4. Implementation of k-NN
5. Implementation of Backpropagation algorithm
6. Comparison of linear regression and decision tree algorithm for the given dataset
7. Comparison of kernel functions of Support Vector Machine for the given dataset

Lecture:45, Practical:30, Total: 75

REFERENCES / MANUALS / SOFTWARES:

1. Ethem Alpaydin, “Introduction to Machine Learning”, 3rd Edition, Prentice Hall of India, 2014.
2. Christopher Bishop, “Pattern Recognition and Machine Learning”, 2nd Edition, Springer, 2011.
3. Willi Richert, Luis Pedro Coelho, “Building Machine Learning Systems with Python”, 2nd Edition, Packt Publishing Ltd., 2015.

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped (Highest Level)**
CO1:	illustrate the foundations of machine learning and apply suitable dimensionality reduction techniques for an application	Applying (K3)
CO2:	make use of supervised methods to solve the given problem	Applying (K3)
CO3:	apply neural networks to solve real world problems	Applying (K3)
CO4:	solve real world problems using kernel machines	Applying (K3)
CO5:	summarize the concepts of reinforcement learning and design machine learning experiments	Analyzing (K4)
CO6:	implement various supervised algorithms and evaluate the performance	Analyzing (K4), Precision (S3)
CO7:	implement the unsupervised algorithms and evaluate the performance	Analyzing (K4), Precision (S3)
CO8:	implement and compare the performance of different algorithms	Analyzing (K4), Precision (S3)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	3		3		
CO2	3		2	2	3
CO3	3		2		3
CO4	3		2		3
CO5	3		2		3
CO6	2		3		2
CO7	2		3		2
CO8	2		3		2

1 – Slight, 2 – Moderate, 3 – Substantial, BT - Bloom’s Taxonomy

18MSE07 BIG DATA ANALYTICS

(Common to Computer Science and Engineering, Information Technology & Information Technology (ICW) branches)

L	T	P	Credit
3	0	2	4

Preamble	Provides basic knowledge about Big data, its framework and storage in databases and prepares the students to perform various analytical operations and visualize the results
Prerequisites	Database Management Systems

UNIT – I 9

Big Data: Definition – Wholeness of big data: Understanding – Capturing –Benefits and management – Organizing and analyzing – Challenges – Big data architecture – Big data sources and applications: Big data sources – Machine to machine Communications- Big data Applications.

UNIT – II 9

MapReduce Framework: Introducing Hadoop – Starting Hadoop – Components of Hadoop: Working with files in HDFS - Anatomy of a MapReduce program – Reading and writing - Writing basic MapReduce programs: Getting the patent data set-Constructing the basic template of a MapReduce program-Counting things-Adapting for Hadoop's API changes-Streaming in Hadoop- Improving performance with combiners – Hadoop Ecosystem.

UNIT – III 9

NoSQL Database Systems: Introduction to NoSQL – CAP theorem - MongoDB : Data types – MongoDB Query Language – Cassandra: Features of Cassandra- Data types – CRUD- Collections Alter Commands – Import and Export- Querying system tables

UNIT – IV 9

Mining Data Streams: Stream Data Model - Sampling Data in a Stream–Filtering Streams–Counting Distinct Elements in a Stream–Estimating Moments–Counting Ones in a Window–Decaying Window - Stream processing with SPARK and Kafka.

UNIT – IV 9

Case Studies: Implement using open source frameworks/tools : Time Series Analysis - Text analysis – Social Network Analysis - Data streams

List of Exercises / Experiments :

1. Install, configure and run Hadoop and HDFS
2. Implement word count / frequency programs using MapReduce
3. Implement an application that stores big data in MongoDB / Cassandra
4. Data streaming using open source frameworks/tools
5. Text Analysis

Lecture:45, Practical:30, Total: 75

REFERENCES/MANUAL/SOFTWARE:

1.	Anil Maheshwari, "Big Data". 1st Edition, McGraw Hill Education, 2017.
2.	Chuck Lam, "Hadoop in Action", 2nd Edition, Manning Publications, 2011.
3.	Seema Acharya and Subhashini Chellappan, "Big Data and Analytics", 1st Edition, Wiley, 2015.
4.	List of Softwares: Hadoop, R Package, Hbase, Pig, Hive

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped** **(Highest Level)**
CO1:	identify the need for big data analytics	Understanding (K2)
CO2:	develop simple programs using Hadoop framework	Understanding (K2)
CO3:	explore NoSQL database system for real world problems	Analyzing (K4)
CO4:	recognize the need for stream processing and discuss SPARK and Kafka architecture	Analyzing (K4)
CO5:	discuss big data use cases and implement using open source frameworks/tools	Applying (K3)
CO6:	demonstrate simple programs using MapReduce, Hadoop and HDFS	Applying (K3), Precision (S3)
CO7:	use MongoDB / Cassandra for storing big data in real world problems	Applying (K3) , Precision (S3)
CO8:	implement programs for data streaming and text analysis using open source frameworks/ tools	Applying (K3) , Precision (S3)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	3		3		
CO2	3		2		3
CO3	3		2		2
CO4	3		2		2
CO5	3		2		2
CO6	2		3		2
CO7	2		3		2
CO8	2		3		2

1 – Slight, 2 – Moderate, 3 – Substantial, BT - Bloom’s Taxonomy

18MIT21 CLOUD ARCHITECTURE AND SECURITY

(Common to Information Technology & Information Technology(Information Cyber Warfare) branches)

L	T	P	Credit
3	0	0	3

Preamble	Provides knowledge about basic concepts of cloud computing, types of cloud services, technologies and service providers and to understand the distinct basic cloud architecture models and advanced architecture models for complex environments and the security issues and threats in cloud environments.
Prerequisites	Nil

UNIT – I **9**

Cloud Computing Basics: Introduction to Cloud Computing – Cloud computing reference model- Essential Characteristics - Benefits and challenges of cloud computing- Roles and Boundaries-Cloud Delivery Models - Deployment models -Cloud computing vendors.

UNIT – II **9**

Cloud Enabling Technology: Data Center Technology-Remote operation and management-Facilities- Computing, Storage, Network Hardware- Virtualization Technology-Types of virtualization- OS based virtualization- Hardware based Virtualization- Virtualization Management-Web Technology- Multitenant Technology- Service Technology- Case Study.

UNIT – III **9**

Fundamental Cloud Architecture: Work load Distribution architecture- Resource Pooling Architecture- Dynamic Scalability-Elastic Resource Capacity-Service load balancing-Redundant Storage Architecture- Case Study.

UNIT – IV **9**

Advanced Cloud Architecture: Hypervisor clustering architecture- Cloud Balancing architecture- Resource Reservation- Dynamic failure detection and recovery architecture-Rapid provisioning- Storage workload management architecture-Multipath resource access architecture-Cross Storage device vertical tiering architecture

UNIT – V **9**

Security in Cloud: Cloud security fundamentals- Basic terms and concepts- Threat agents- Cloud Security Threats-Encryption- Hashing- Digital Signature-Public Key Infrastructure- Identity and Access Management- Single Sign on-Cloud Based Security Groups.

Total: 45

REFERENCES:

1. Thomas Erl, Zaigham Mahmood, Ricardo Puttini, “Cloud Computing: Concepts, Technology and Architecture”, 1st Edition, Prentice Hall, 2013.
2. Anthony T. Velte, Toby J. Velte, Robert Elsenpeter, “Cloud Computing: A Practical Approach”, 1st Edition, McGraw-Hill, 2010.
3. George Reese, “Cloud Application Architectures: Building Applications and Infrastructure in the Cloud”, 1st Edition, O'Reilly, 2009.

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped** **(Highest Level)**
CO1:	articulate the main concepts, key technologies, strengths and limitations of cloud computing	Understanding (K2)
CO2:	illustrate the architecture, infrastructure and delivery models of cloud computing	Understanding (K2)
CO3:	analyze the different cloud technologies including virtualization and web based technologies	Analyzing (K3)
CO4:	categorize the appropriate cloud architecture for distinct functional areas.	Analyzing (K3)
CO5:	identify the core issues of cloud computing such as security, threats and privacy.	Understanding (K2)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	2	2	1	1	2
CO2	2	2		1	2
CO3	3	3		3	3
CO4	3	3			3
CO5	3	2	3	1	2

1 – Slight, 2 – Moderate, 3 – Substantial, BT – Bloom’s Taxonomy

18MIE04 MOBILE AND WIRELESS SECURITY

(Common to Information Technology &
Information Technology(Information Cyber Warfare) branches)

L	T	P	Credit
3	0	0	3

Preamble	The objective of this course is to have better knowledge on security issues, applications, attacks and security issues in wireless and mobile communications.
Prerequisites	Computer Networks

UNIT – I **9**

Introduction to Mobile and Wireless Networks: Cellular Networks, 1G through 3G, IEEE Networks - WLAN IEEE 802.11, WPAN IEEE 802.15, WMAN IEEE 802.16, IEEE 802.20, MIH IEEE 802.21, WRAN IEEE 802.22, Mobile Internet Networks – Macro and Micro mobility – Personal mobility – SIP – Identity based mobility, NEMO and MANETs – Vulnerabilities in wireless communications –security basics – symmetric and asymmetric cryptography, Hash functions – Electronic signatures – MAC – PKI and electronic certificate – IPSec – AAA protocol – Firewalls – Intrusion detection.

UNIT – II **9**

Wi-Fi Security Architectures: Hot Spot architecture – WIDS – Rogue AP detection – IEEE 802.11 geolocation techniques – Honeypots –Bluetooth Security – Protocol architecture – Radio physical layer – Device addressing – SCO and ACL logical transports – Security mode – Authentication and pairing – Attacks – BlueSmack – WiFi Security-Passive and Active attacks – DOS attacks – Trojan attack – Dictionary Attack.

UNIT – III **9**

IEEE 802.11 and WiMaX Security: Security in IEEE 802.11 – WEP – WEP2 – IV collisions – RC4 weakness – 802.1x authentication - 802.11i security architecture – policy negotiation – radio security policies – RADIUS – EAP – PKI – WiMAX security – TEK – KEK – IEEE 802.16e – PKMv2-RSA – Security Association – 3 way handshake – role of smart cards in WiMAX.

UNIT – IV **9**

Security in Adhoc Networks: Attacks to routing protocols – Security mechanisms – Auto-configuration – Key management – Self-managed PKI – Resurrecting Duckling – Group key management – Wireless Sensor Networks – Attacks – Preventive mechanisms – Intrusion tolerance – SNEP - µTELSA – TinySec – key management in WSNs.

UNIT – V **9**

Security in Mobile Telecommunication Networks: Signaling system 7 (SS7) – GSM security – GRPS security – UMTS infrastructure and security – H.323 – SIP – Megaco – VoIP security flaws and countermeasure – IMS architecture – security flaws – 4G security – Protection of interception – Security issues in Mobile IP – HIP – NetLMM.

Total: 45

REFERENCES:

1. Hakima Chaouchi and Maryline Laurent-Maknavicius, "Wireless and Mobile Network Security: Security basics, Security in On-the-shelf and Emerging Technologies", 2nd Edition, John Wiley & Sons, 2009.
2. Pallapa Venkataram and Sathish Babu, "Wireless and Mobile Network Security", 1st Edition, Tata McGraw Hill, 2010.
3. Amitabh Mishra, "Security and Quality of Service in Ad Hoc and Wireless Networks", 1st Edition, Cambridge University Press, 2008.

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped (Highest Level)**
CO1:	describe the physical and logical design of IoT and identify the appropriate IoT level and develop design methodologies for a given application	Applying (K3)
CO2:	explain the architecture, need for middleware and the role of different standardization protocols	Understanding (K2)
CO3:	recall the basic concepts and packages of Python related to IoT for interfacing with IoT devices	Applying (K3)
CO4:	develop simple real time applications, upload the data onto the cloud and perform data analytics	Applying (K3)
CO5:	identify the security threats against a given IoT system and suggest simple countermeasures	Understanding (K2)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	2		2	2	
CO2	3		3	3	1
CO3	3		3	3	1
CO4	3		3	3	2
CO5	2		3	3	3

1 – Slight, 2 – Moderate, 3 – Substantial, BT – Bloom’s Taxonomy

18MWE01 SECURED NETWORK PROTOCOLS

L	T	P	Credit
3	0	0	3

Preamble	To acquire the knowledge on the various network protocols to provide the more security for the communication network and the data transmitted over the network.
Prerequisites	Network Protocols, Computer Networks

UNIT – I **9**

Local Area Network and LAN Protocols: ETHERNET Protocols – VLAN protocols – Wireless LAN Protocols – Metropolitan Area Network Protocol – Storage Area Network and SAN Protocols – FDMA, WIFI and WIMAX Protocols- security issues, Mobile IP – Mobile Support Protocol for Ipv4 and Ipv6 – Resource Reservation Protocol, Multi-casting Protocol – VGMP – IGMP – MSDP

UNIT – II **9**

Network Security and Technologies and Protocols: AAA Protocols – Tunneling Protocols – Secured Routing Protocols – GRE- Generic Routing Encapsulation – IPSEC – Security architecture for IP – IPSECAH – Authentication Header – ESP – IKE – ISAKMP and Key management Protocol, IEEE 802.11 – Structure of 802.11 MAC – WEP- Problems with WEP – Attacks and Risk- Station security – Access point Security – Gate way Security – Authentication and Encryption.

UNIT – III **9**

Authentication and Network Security: Authentication requirements – Authentication functions – Message Authentication Codes – Hash Functions – Security of Hash Functions and MACs – MD5 message Digest algorithm – Secure Hash Algorithm – RIPEMD – HMAC- Authentication Applications: Kerberos – X.509 Authentication Service.

UNIT – IV **9**

Security Protocols: Transport layer protocols – SSL – Electronic mail security – PEM and S/MIME security protocol – Pretty Good Privacy – Web Security – Firewalls design principles –Trusted systems – Electronic payment protocols, Intrusion detection – password management – Viruses and related Threats – Virus Counter measures, Virtual Private Networks.

UNIT – V **9**

IEEE 802.15 and Bluetooth: WPAN Communication Protocols – IEEE 802.16- IEEE 802.16AWCDMA – Services – WCDMA Products – Networks- device addressing – System Addressing – Radio Signaling Protocol – Multimedia Signaling Protocol- Global Mobile Satellite Systems : Case studies of the IRIDIUM and GLOBALSTAR systems- Wireless Enterprise Networks: Introduction to Virtual Networks, Bluetooth technology, Bluetooth Protocols.

Total: 45

REFERENCES:

1. William Stallings, “Cryptography and Network Security: Principles and Standards”, Prentice Hall India, 4th Edition, 2009.
2. Bruce Potter and Bob Fleck, “802.11 Security”, O’Reilly Publications, 2002.
3. Lawrence Harte, “Introduction to CDMA- Network services Technologies and Operations”, Althos Publishing, 2004.

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped (Highest Level)**
CO1:	apply the basic security algorithms required by any computing system	Applying (K3)
CO2:	predict the vulnerabilities across any computing system and hence be able to design a security solution for any computing system	Applying (K3)
CO3:	implement the authentication between the sender and receiver	Applying (K3)
CO4:	develop an security mechanism for mail and web applications	Applying (K3)
CO5:	address the problems and vulnerabilities of wireless network	Applying (K3)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1		1	2	1	3
CO2	1		2	2	3
CO3			1	2	2
CO4	3		3	2	2
CO5	2		2	2	2

1 – Slight, 2 – Moderate, 3 – Substantial, BT - Bloom’s Taxonomy

18MWE02 INFORMATION THEORY AND CODING

(Common to Information Technology (Information Cyber Warfare), Information Technology & Communication Systems branches)

L	T	P	Credit
3	0	0	3

Preamble	Information Theory and Coding deals with concept of information and its efficient, error-free and secure delivery of information using binary data streams. It also provides a complete understanding of error-control coding techniques over noisy communication channel.
Prerequisites	Communication Networks/Systems

UNIT – I 9

Source Coding: Introduction to Information theory – Uncertainty and Information – Entropy and Average Mutual Information – Information Measure for Continuous Random Variables – Source coding theorem – Huffman Coding – Shannon-Fano-Elias Coding – Arithmetic Coding – Lempel – Ziv Algorithm – Run Length Encoding and the PCX Format – Rate Distortion Function

UNIT – II 9

Channel Capacity and Coding: Introduction – Channel Model – Channel Capacity – Channel Coding – Information Capacity Theorem – Error control coding: Introduction to Error Correction Codes – Basic Definitions – Matrix Description of Linear Block Codes – Equivalent Codes – Parity Check Matrix – Decoding of Linear Block Code – Syndrome Decoding – Error Probability after Coding – Perfect Codes – Hamming Codes – Low Density Parity Check (LDPC) Codes – Optimal Linear Codes – Maximum Distance Separable (MDS) Codes

UNIT – III 9

Cyclic Codes: Introduction to the Cyclic Codes – Polynomials – Division Algorithm for Polynomials – A Method for Generating Cyclic Codes – Matrix Description of Cyclic Codes – Burst Error Correction – Fire Codes – Golay Codes – Cyclic Redundancy Check (CRC) Codes – Circuit Implementation of Cyclic Codes

UNIT – IV 9

Bose-Chaudhuri Hocquenghem (BCH) Codes: Introduction to BCH Code – Primitive Elements – Minimal Polynomials – Generator Polynomials in Terms of Minimal Polynomials – Some Examples of BCH Codes – Decoding of BCH codes – Reed-Solomon Codes – Implementation of Reed –Solomon Encoders and Decoders – Performance of RS Codes Over Real Channels – Nested Codes

UNIT – V 9

Convolutional Codes: Introduction to Convolutional Codes – Tree Codes and Trellis Codes – Polynomial Description of Convolution Codes – Distance Notions for Convolutional Codes – The Generating Function – Matrix Description of Convolutional Codes – Viterbi Decoding and Convolutional Codes – Distance Bounds for Convolutional Codes – Turbo Codes

Total: 45

REFERENCES:

1. Ranjan Bose, “Information Theory, Coding and Cryptography”, 2nd Edition, Tata McGraw Hill, 2008.
2. Andrew J. Viterbi, Jim K. Omura, “Principles of Digital Communication and Coding”, 4th Edition, Courier Corporation, 2018.
3. John G. Proakis, Masoud Salehi, “Digital Communications”, 5th Edition, McGraw Hill, 2008.

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped (Highest Level)**
CO1:	outline the principles behind an efficient, correct and secure transmission of digital data stream	Understanding (K2)
CO2:	recognize the basics of error-coding techniques	Analyzing (K4)
CO3:	construct the knowledge about the encoding and decoding of digital data streams	Applying (K3)
CO4:	examine the performance requirements of various coding techniques	Analyzing (K4)
CO5:	take part in to conduct research in information theory by the professionals	Evaluating (K5)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	2		3	2	2
CO2	2		3		2
CO3			2	3	1
CO4	3	2		2	1
CO5	3		2	1	2

1 – Slight, 2 – Moderate, 3 – Substantial, BT - Bloom’s Taxonomy

18MWE03 MULTIMEDIA COMPRESSION TECHNIQUES

(Common to Information Technology (Information and Cyber Warfare), Information Technology & Communication Systems branches)

L	T	P	Credit
3	0	0	3

Preamble	The aims of this course are to study methods for handling and compressing various kinds of data, such as text, images, audio and video data and understand data compression techniques for multimedia and other applications, in particular to the Internet.
Prerequisite	Computer Networks

UNIT – I **9**

Introduction: Special features of Multimedia – Graphics and Image Data Representations – Popular File formats – Fundamental Concepts in Video – Digital Audio – Storage requirements for multimedia applications –Need for Compression – Lossy & Lossless compression techniques– Overview of Source Models – Source coding – Scalar and Vector quantization

UNIT – II **9**

Text Compression: Compression techniques: Shannon- Fano coding –Huffman coding – Adaptive Huffman Coding – Arithmetic coding – Dictionary techniques: LZW algorithm

UNIT – III **9**

Audio Compression: Audio compression techniques – μ- Law and A-Law companding- Differential Encoding –DPCM- ADPCM – DM – Optimal Predictors and Optimal Quantization –Application to speech coding: G.722 – Application to audio coding : MPEG audio, Speech compression techniques : Formants and CELP Vocoders

UNIT – IV **9**

Image Compression : Transform Coding: JPEG Standard – Sub band coding algorithms – Design of Filter banks – Implementation using filters- Wavelet based compression: EZW- SPIHT coders – JPEG 2000 standards- JBIG- JBIG2 standards

UNIT – V **9**

Video Compression: Video compression Based on Motion Compensation – Search for Motion Vectors – H.261 – MPEG Video Coding I: MPEG – 1 and 2 – MPEG Video Coding II: MPEG – 4: Object Based Visual Coding –Synthetic Object Coding –Object types-Profiles and Levels – MPEG 7.

Total: 45

REFERENCES:

1. Morgan Kauffman, Khalid Sayood, “Introduction to Data Compression”, 2nd Edition, Harcourt India, 2000.
2. David Salomon, “Data Compression – The Complete Reference”, 2nd Edition, Springer Verlag New York Inc., 2001.
3. Mark S. Drew, Ze-Nian Li, “Fundamentals of Multimedia”, 2nd Edition, PHI, 2005.

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped (Highest Level)**
CO1:	summarize scalar and vector quantization theory and also to represent the multimedia data in different formats for various applications	Understanding (K2)
CO2:	make use of different coding techniques and apply various algorithms for text compression	Applying (K3)
CO3:	identify the various audio and speech compression techniques for practical applications	Applying (K3)
CO4:	take part in image compression techniques and also to implement the compression techniques in MATLAB	Analyzing (K4)
CO5:	compare various video compression algorithms for practical applications	Evaluating (K5)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	3	2	2		
CO2	3		2		3
CO3	2	1	3	1	
CO4	2		2	3	1
CO5	3		2	1	2

1 – Slight, 2 – Moderate, 3 – Substantial, BT - Bloom’s Taxonomy

18MWE04 ADVANCED OPERATING SYSTEMS AND SECURITY

L	T	P	Credit
3	0	0	3

Preamble	This course is intended to give students a thorough understanding of design and implementation issues for modern operating systems and cover key design issues in implementing an operating system, such as resource management, synchronization, load sharing, inter-process communication, deadlock and paying particular attention to system security and security in Linux and Windows.
Prerequisites	Operating System basics

UNIT – I **9**

Distributed Operating System: Architecture of distributed systems-Theoretical foundations: Inherent Limitations of a Distributed System – Lamport's Logical clocks – Vector Clocks – Casual Ordering of Messages – Global State – Cuts of a Distributed Computation – Termination Detection-Distributed mutual exclusion –Distributed deadlock detection-agreement protocols: The System Model – A Classification of Agreement Problems – Solutions to the Byzantine Agreement Problem – Applications of Agreement Algorithms.

UNIT – II **9**

Distributed Resource Management: Distributed file systems – Architecture – Mechanisms for Building Distributed File Systems – Design Issues – Case Studies – Log-Structured File Systems-Distributed shared memory**:** Architecture and Motivation – Algorithm for Implementing DSM – Memory Coherence Protocols – Design Issues – Case Studies-Distributed scheduling**:** Motivation – Issues in Load Distributing – Components of a Load Distributing Algorithm – Stability – Load Distributing Algorithm – Performance Comparison – Selecting a Suitable Load Sharing Algorithm – Requirements for Load Distributing – Load Sharing Policies – Task Migration – Issues in Task Migration.

UNIT – III **9**

Failure Recovery and Fault Tolerance: Basic Concepts – Classification of Failures – Backward and Forward Error Recovery – Backward Error Recovery :Basic Approaches – Recovery in Concurrent Systems – Consistent Set of Check points – Synchronous Check pointing and Recovery – Asynchronous Check pointing and Recovery – Check pointing for Distributed Database Systems – Recovery in Replicated Distributed Database Systems-Fault tolerance: Issues – Atomic Actions and Committing – Commit Protocols – Non-blocking Commit Protocols – Voting Protocols – Dynamic Voting Protocols – The Majority based Dynamic Voting Protocols – Failure Resilient Processes – Reliable Communication.

UNIT – IV **9**

Trust in Secure Operating Systems: Secure operating systems- Security goals- Trust model- Threat model-Access Control fundamentals: Lampson's access matrix, mandatory protection systems, Reference monitor-Secure operating system definition-Assessment criteria.

UNIT – V **9**

Operating System Security: Security in Windows and Unix: Protection system, authorization, security analysis and vulnerabilities- The security kernel- Secure communications processor – Retrofitting security into operating systems – Windows 7 Security.

Total: 45

REFERENCES:

1. Mukesh Singhal, "Advanced concepts in operating systems", Tata McGraw Hill, 2008.
2. Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, "Operating System Concepts", 7th Edition, John Wiley & Sons, 2004.
3. Trent Jaeger, "Operating Systems Security", Morgan & Claypool Publishers, 2008
4. Michael J. Palmer, "Guide to Operating Systems Security", Thomson/Course Technology, 2004.

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped** **(Highest Level)**
CO1:	identify the various process synchronization mechanisms and demonstrate the distributed mutual exclusion algorithms deadlock detection and agreement protocols of distributed operating system	Understanding (K2)
CO2:	investigate various resource management techniques for distributed systems	Applying (K3)
CO3:	illustrate various failure recovery and fault-tolerant techniques and issues	Understanding (K2)
CO4:	investigate the methods for secure operating systems	Applying (K3)
CO5:	investigation for providing security in Unix and windows	Applying (K3)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	2		2	1	1
CO2	2	2	2	1	1
CO3	2	2	2	2	2
CO4	3	3	3	3	3
CO5	3	3	3	3	3

1 – Slight, 2 – Moderate, 3 – Substantial, BT - Bloom’s Taxonomy

18MWE05 UNIX INTERNALS

L	T	P	Credit
3	0	0	3

Preamble	To gain the concepts of UNIX Operating system to recognize various issues in process management, buffer representation, kernels and system calls. Alongside, it gives an insight about various memory management policies like segmentation, paging and I/O subsystems
Prerequisites	Nil

UNIT – I		**9**

Overview: General Overview of the System: History – System structure – User perspective – Operating system services – Assumptions about hardware. Introduction to the Kernel : Architecture of the UNIX operating system – Introduction to system concepts. The Buffer Cache: Buffer headers – Structure of the buffer pool – Scenarios for retrieval of a buffer – Reading and writing disk blocks – Advantages and disadvantages of the buffer cache.

UNIT – II		**9**

File System: Internal representation of files: Inodes – Structure of a regular file – Directories – Conversion of a path name to an Inode – Super block – Inode assignment to a new file – Allocation of disk blocks

UNIT – III		**9**

System calls for the File System: Open – Read – Write – File and record locking – Adjusting the position of file I/O – Lseek – Close – File creation – Creation of special files – Changing directory, root, owner, mode – stat and fstat – Pipes – Dup – Mounting and unmounting file systems – link – unlink.

UNIT – IV		**9**

Process: Process states and transitions – Layout of system memory – The context of a process – Saving the context of a process – Manipulation of the process address space – Sleep. Process Control : Process creation – Signals – Process termination – Awaiting process termination – Invoking other programs – user id of a process – Changing the size of a process – Shell – System boot and the INIT process– Process Scheduling.

UNIT – V		**9**

Memory Management and I/O: Memory Management Policies- Swapping – Demand paging. The I/O Subsystem: Driver Interface – Disk Drivers – Terminal Drivers– Streams – Inter process communication.

Total: 45

REFERENCES:

1. Maurice J. Bach, “The Design of the Unix Operating System”, 1st Edition, Pearson Education, 2006.
2. https://goo.gl/p5f5KH
3. Goodheart B., Cox J., “The Magic Garden Explained”, Prentice Hall of India, 1994.
4. Leffler S. J., Mckusick M. K., Karels M. J. and Quarterman J. S., “The Design and Implementation of the 4.3 BSD Unix Operating System”, Addison Wesley, 1998.

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped (Highest Level)**
CO1:	operate UNIX systems and shell programming	Understanding (K2)
CO2:	analyze the buffers and kernel representation	Applying (K3)
CO3:	examine the UNIX system structure and system calls	Analyzing (K4)
CO4:	trace and examine various processes	Analyzing (K4)
CO5:	examine the memory management and interprocess communication	Analyzing (K4)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1				3	2
CO2	3	2		3	
CO3		3	3		
CO4	3	2	3		2
CO5	3	2	3		2

1 – Slight, 2 – Moderate, 3 – Substantial, BT - Bloom’s Taxonomy

18MWE06 INTRUSION DETECTION

L	T	P	Credit
3	0	0	3

Preamble	To understand model of intrusion analysis and give a brief description of security design principles
Prerequisites	Cryptography and network security

UNIT – I **9**

Introduction: Defining Intrusion Detection - The history of intrusion and Detection- Audit: Setting - The Stage for Intrusion Detection- The birth of intrusion Detection- Security concepts intrusion Detection concept-Determining strategies for Intrusion Detection

UNIT – II **9**

Information Sources: Host based information sources-Network based information sources-Information other security products-Analysis Scheme: A model for intrusion Analysis,-Techniques

UNIT – III **9**

Responses and Vulnerability Analysis: Requirement of Responses-Types of responses-covering tracks during investigation- mapping responses of Policy- Vulnerability Analysis-Credentialed approaches -Technical issues

UNIT – IV **9**

Real-World Challenge and Legal Issues: Roots of Security Problem-Hacker-Rules for Intrusion Detection System-Law for Geeks- Rules of Evidence- Laws related to Monitoring Activity- Building Case for security

UNIT – V **9**

For designer: Requirement- Security Design principles - Surviving the designing process - Future trends in technology- a vision for intrusion Detection

Total: 45

REFERENCES:

1. Rebecca Gurley Bace, “Intrusion Detection”, 1st Edition, Macmillan Technical Publishing, 2000.
2. Stephen Northcutt and Jady Novak, “Network Intrusion Detection”, 3rd Edition, New Riders Publishing, 2003.
3. Carol Fung and Raouf Boutaba, “Intrusion Detection Networks” ,1st Edition, Auerbach Publication, 2017.

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped** **(Highest Level)**
CO1:	explain a network intrusion detection system	Understanding (K2)
CO2:	develop predictive measures to assess and prevent intrusion	Understanding (K2)
CO3:	assess implications of privacy, security, and ethical issues as they pertain to an organization's IT infrastructure	Understanding (K2)
CO4:	diagnose possible hacks and propose policies to outline what do when an intrusion occurs	Applying (K3)
CO5:	evaluate physical solutions for preventing intrusion	Applying (K3)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	2	1	2	2	
CO2	2	-	2	2	1
CO3	3	2	2	2	1
CO4	3	1	2	2	1
CO5	2	1	2	2	1

1 – Slight, 2 – Moderate, 3 – Substantial, BT - Bloom’s Taxonomy

18MWE07 STEGANOGRAPHY AND DIGITAL WATERMARKING

L	T	P	Credit
3	0	0	3

Preamble	To make the students familiar about digital watermarking and steganography and should be able understand how digital watermarking and steganography works and how can they be used in applications for making it more secure
Pre-requisites	Network Security

UNIT – I 9

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

UNIT – II 9

Steganography: Survey of steganographic techniques – Substitution system and bitplane tools – Transform domain techniques – Spread spectrum and Information hiding – Statistical Steganography - Distortion and Code generation techniques – Automated generation of English text.

UNIT – III 9

Steganalysis and Watermarking: Introduction and terminology - Detecting hidden information – Extracting hidden information - Disabling hidden information – Watermarking: Introduction – History and terminology - Watermarking Principles – Applications – Requirements of algorithmic design issues – Evaluation and Benchmarking of watermarking system.

UNIT – IV 9

Survey of Current Watermarking Techniques: Cryptographic and psycho visual aspects – Choice of a workspace – Formatting the watermark bits - Merging the watermark and the cover – Optimization of the watermark receiver – Extension from still images to video – Robustness of copyright making systems: Robustness requirements – signal diminishment – Watermark detector failure – counterfeiting marks – detection of the watermark – system architecture issues – court of law attacks.

UNIT – V 9

Fingerprints: Examples – Classification – Research History – Fingerprinting Schemes – Digital copyright and Watermarking – Conflict of copyright laws on the internet.

Total: 45

REFERENCES:

1. Stefan Katzenbelsser and Fabien A. P. Petitcolas, “Information hiding techniques for Steganography and Digital Watermarking”, 1st Edition, ARTECH House Publishers, 2004.
2. Jessica Fridrich, “Steganography in Digital Media: Principles, Algorithms, and Applications”, 1st Edition, Cambridge University Press, 2010.
3. Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich and Ton Kalker, “Digital Watermarking and Steganography”, 1st Edition, Morgan Kaufmann Publishers, 2007.

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped (Highest Level)**
CO1:	know the history and importance steganography and watermarking	Understanding (K2)
CO2:	identify theoretic foundations of steganography	Understanding (K2)
CO3:	expose to various scenarios of steganalysis	Applying (K3)
CO4:	design a new/existing security methods	Applying (K3)
CO5:	compare and realize new/existing hiding techniques	Analyzing (K4)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	1	3	2		2
CO2	1	2	3		2
CO3			2	3	3
CO4	3	1	2		3
CO5	1	1	2	3	3

1 – Slight, 2 – Moderate, 3 – Substantial, BT - Bloom’s Taxonomy

18MWE08 VIDEO ANALYTICS

L	T	P	Credit
3	0	0	3

Preamble	The objective of this course is to enrich the knowledge about video processing, data analytics, video content analysis in real-time and studies of video analytics.
Prerequisites	Computer Networks

UNIT – I **9**

Video Fundamentals: Basic concepts and Terminology-Monochrome Analog video – Color in Video – Analog video standards – Digital video basics – Analog-to Digital conversion – Color representation and chroma sub sampling – Digital video formats and standards Video sampling rate and standards conversion.

UNIT – II **9**

Video Segmentation and Video Features: Fundamentals of Motion Estimation – Optical flow - Pixel Video Features - colour, shape features, Textural features - Feature selection and Dimensionality Reduction.

UNIT – III **9**

Introduction to Analytics: Big-Data - Descriptive data analysis - Analytic Processes and Tools - Regression - Classification - Clustering algorithms - Validation - Multimodal approach to Image and Video data mining - Probabilistic semantic mode - Model based annotation and video mining.

UNIT – IV **9**

Video Content Analysis and Analytics: Introduction- Detecting Shot Boundaries in Video – Parsing a Video into Semantic Segments – Video Indexing and Abstraction for Retrievals – Affective Video Content Analysis - Automatic Video Trailer Generation - Video database - Video categorization - Video query categorization.

UNIT – V **9**

Emerging Trends: Object Segmentation and Tracking in the Presence of Complex Background – Video Inpainting – Video Summarization – Forensic video analysis.

Total: 45

REFERENCES:

1. Oges Marques, "Practical Image and Video Processing Using MATLAB", 1st Edition, Wiley-IEEE Press, 2011.
2. Michael Berthold, David J.H and, "Intelligent Data Analysis", 2nd Edition, Springer, 2007.
3. Anand Rajaraman and Jeffrey David Ullman, "Mining of Massive Datasets", 2nd Edition ,Cambridge University Press, 2014.

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped (Highest Level)**
CO1:	explain video processing fundamentals	Understanding (K2)
CO2:	identify the motion and video features	Applying (K3)
CO3:	illustrate about data analytics and video mining	Applying (K3)
CO4:	examine various video segments and database	Applying (K3)
CO5:	analyze the recent trends of video analysis	Analyzing (K4)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	2		2	3	
CO2	3		1	1	
CO3	2		2	3	2
CO4	2		2	2	
CO5	3			2	2

1 – Slight, 2 – Moderate, 3 – Substantial, BT - Bloom’s Taxonomy

18MWE09 WEB APPLICATION SECURITY

L	T	P	Credit
3	0	0	3

Preamble	Identify various components of an web application from the security view point and impart the knowledge of web application testing methodologies by examining the principles of securing common area of functionality of web application.
Prerequisites	Web Technology

UNIT – I **9**

Security Fundamentals and Security Principles: Web Security Fundamentals- Input Validation, Attack surface reduction, classifying and prioritizing threads, Authentication-Securing Password, Best Practices, Authorization-Access control - Session Management - securing web application

UNIT – II **9**

Browser and Database Security Principles: Browser security principles- cross-site scripting - cross-site request forgery- Database security principles – SQL injection- setting database permission-stored procedure security- Insecure Direct object references

UNIT – III **9**

File security and Security Methodologies: File security principles- source code secret- forceful browsing- directory traversal- secure development methodologies- application security - industry standard secure development methodologies and maturity models - SDL - CLASP- SAMM - BSIMM.

UNIT – IV **9**

Web Testing Fundamentals: Web Applications Testing Fundamentals- Basic Observation HTML Page Source-Viewing a Page's HTML Source, Advanced -Observing Live Request Headers with Firebug - Observing Live Post Data with Web Scarab - Seeing Hidden Form Fields - Observing Live Response Headers with Tamper Data- Web-Oriented Data Encoding.

UNIT – V **9**

Bypass client-side input validation and Session Manipulation: Automating with LibWWW-Perl, Seeking Design Flaws, Attacking AJAX, Manipulating Sessions -Finding Session Identifiers in Cookies - Finding Session Identifiers in Requests - Finding Authorization Headers - Analyzing Session ID Expiration - Analyzing Session Identifiers with Burp

Total: 45

REFERENCES:

1. Bryan Sullivan, Vincent Liu, "Web Application Security- A Beginner's Guide", 1st Edition, McGraw-Hill Education, 2011.
2. Paco Hope, Ben Walther, "Web Security Testing Cookbook", 1st Edition, O'Reilly Media, 2008.
3. Georgia Weidman, "Penetration Testing: A Hands-On Introduction to Hacking", 1st Edition, No Starch Press, 2014.

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped (Highest Level)**
CO1:	explain primer on web security fundamentals, authentication and authorization	Understanding (K2)
CO2:	describe principles of browser security, database security and file security	Understanding (K2)
CO3:	identify approaches for security development methodologies	Applying (K3)
CO4:	determine the observations behind the façade of web application to test the functionality and data encoding	Analyzing (K4)
CO5:	demonstrate various testing techniques for web application	Applying (K3)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	2		2		
CO2	2			2	1
CO3	2		3	2	
CO4		2		2	2
CO5	1		2	2	2

1 – Slight, 2 – Moderate, 3 – Substantial, BT - Bloom’s Taxonomy

18MWE10 GAME THEORY AND ITS APPLICATIONS

L	T	P	Credit
3	0	0	3

Preamble	Explore the basic concepts of game theory, non-cooperative solutions, and cooperative solutions. Designing sequential games and application oriented games.
Prerequisites	Nil

UNIT – I **9**

Fundamentals: Conflict– Strategy and Games – Game theory – The Prisoner’s Dilemma– Scientific metaphor– Business case– Games in normal and extensive forms – Representation– Examination – Examples.

UNIT – II **9**

Non Cooperative Equilibria in Normal Games: Dominant Strategies and Social Dilemmas– Nash Equilibrium– Classical Cases in Game theory– Three person games– Introduction to Probability and Game theory– N– Person games.

UNIT – III **9**

Cooperative Solutions: Elements of Cooperative Games– Credible commitment– A Real Estate Development– Solution Set– Some Political Coalitions– Applications of the Core to Economics – The Market Game– The Core of a Two Person Exchange Game– The Core with More than Two Pairs of Traders– The core of Public Goods Contribution Game– Monopoly and Regulation.

UNIT – IV **9**

Sequential Games: Strategic Investment to Deter Entry– The Spanish Rebellion– Again– Imbedded Games – Planning Doctoral Study– Centipede Solved– Repeated play– Campers Dilemma– Pressing the shirts– Indefinitely Repeated Play – A Repeated Effort Dilemma

UNIT – V **9**

Applications: Voting Games– Games and Experiments– Auctions– Evolution and Boundary Rational Learning – Case studies of Wireless Networks and Applications

Total: 45

REFERENCES:

1. Roger A. McCain, “Game Theory – A Non– Technical Introduction to the Analysis of Strategy”, 3rd Edition, World Scientific Publishers, 2010.
2. Drew Fudenberg and Jean Tirole, “Game Theory”, 1st Edition, MIT Press, 1991.
3. Osborne, “An Introduction to Game Theory”, 1st Edition, Oxford University Press, 2012.

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped** **(Highest Level)**
CO1:	explain the various algorithms in game theory	Understanding (K2)
CO2:	interpret the non co operative solutions for games.	Understanding (K2)
CO3:	apply the cooperative solutions in game design	Applying (K3)
CO4:	demonstrate sequential gaming techniques	Applying (K3)
CO5:	develop game applications	Applying (K3)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	2	2		1	
CO2		2	1		
CO3	2	2	2		2
CO4		2		2	2
CO5	2	3	2	3	2

1 – Slight, 2 – Moderate, 3 – Substantial, BT - Bloom’s Taxonomy

18MWE11 BIOMETRIC SECURITY

L	T	P	Credit
3	0	0	3

Preamble	Biometric Security is mainly deals with the fundamental knowledge about biometrics, and standards applied to security and different types biometric technologies with strengths and weaknesses
Pre-requisites	Nil

UNIT – I 9

Biometrics: Introduction- Benefits of biometrics over traditional authentication systems –Benefits of biometrics in identification systems-Selecting a biometric for a system –Applications – Key biometric terms and processes - Biometric matching methods -Accuracy in biometric systems

UNIT – II 9

Facial and Fingerprint Biometric Technologies: Fingerprints - Technical description – Characteristics - Competing technologies - Strengths – Weaknesses – Deployment - Facial scan – Technical description - Characteristics - Weaknesses-Deployment.

UNIT – III 9

Physiological Biometric Technologies: Iris scan - Technical description – Characteristics - Strengths – Weaknesses – Deployment - Retina vascular pattern – Technical description – Characteristics - Strengths – Weaknesses – Deployment - Hand scan – Technical description-Characteristics - Strengths – Weaknesses deployment – DNA biometrics

UNIT – IV 9

Behavioral Biometric Technologies: Handprint Biometrics - DNA Biometrics - Signature and Handwriting technology - Technical description – Classification - Keyboard / Keystroke dynamics - Voice – Data acquisition - Feature extraction - Characteristics - Strengths – Weaknesses- Deployment.

UNIT – V 9

Multi Biometrics: Multi biometrics and multi factor biometrics - Two-factor authentication with passwords - Tickets and Tokens – Executive decision - Implementation plan-Case studies on Physiological, Behavioral and Multifactor biometrics in identification systems.

Total : 45

REFERENCES:

1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi, “Biometrics -Identity verification in a network”, 1st Edition Reprint, Wiley Eastern, 2012.
2. John Chirillo and Scott Blaul, “Implementing Biometric Security”, 1st Edition, Wiley Eastern Publications, 2005.
3. John Berger, “Biometrics for Network Security”, 1st Edition, Prentice Hall, 2004.

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped (Highest Level)**
CO1:	explain the basic principles and terminologies behind biometric systems	Understanding (K2)
CO2:	analyze the characteristics of physical and physiological biometric technologies	Applying (K3)
CO3:	describe and Classify the different types of behavioral biometric technologies	Understanding (K2)
CO4:	summarize the significance of multi biometrics	Understanding (K2)
CO5:	select the suitable biometric technology based on the security applications	Analyzing (K4)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1		3	3		3
CO2	3			3	
CO3		3		3	2
CO4	3		3	3	3
CO5	3	3		3	3

1 – Slight, 2 – Moderate, 3 – Substantial, BT - Bloom's Taxonomy

18MWE12 CYBER PHYSICAL SYSTEMS

(Common to Information Technology(ICW) & Mechatronics branches)

L	T	P	Credit
3	0	0	3

Preamble	This subject strives to identify and introduce the durable intellectual ideas of embedded systems as a technology and as a subject of study. The emphasis is on modeling, design, and analysis of cyber-physical systems, which integrate computing, networking, and physical processes
Prerequisites	Nil

UNIT – I **9**

Cyber Physical Systems: Introduction- Applications -Modeling dynamic behaviors –continue dynamics – Newtonian mechanics – actor models – properties of systems – feedback control-Discrete dynamics: discrete systems – the notion of state – finite-state machines – extended state machines – non determinism – behaviors and traces

UNIT – II **9**

Hybrid Systems: Modal models – classes of hybrid systems-Composition of state machines: concurrent composition – hierarchical state machines-Concurrent models of computation: structure of models – synchronous-reactive models – dataflow models of computation – timed models of computation

UNIT – III **9**

Design of Embedded Systems: Embedded processors: types of processors – parallelism-Memory architectures: memory technologies – memory hierarchy – memory models-Input and output: i/o hardware – sequential software in a concurrent world – the analog digital interface-Multi Tasking: Imperative programs – threads – processes and message processing- Scheduling : basics of scheduling – rate monotonic scheduling – earliest deadline first – scheduling and mutual exclusion – multiprocessor scheduling

UNIT – IV **9**

Analysis and Verification: Invariants and temporal logic: invariants – linear temporal logic-Equivalence and refinement: models as specifications – type equivalence and refinement – language equivalence and containment – simulation – bisimulation- Reachability analysis and model checking: open and closed systems – reach ability analysis – abstraction in model checking – model checking liveness properties

UNIT – V **9**

Quantitative Analysis: Problems of internet – programs as graphs – factors determining execution time – basics of execution time analysis – other quantitative analysis problems- Sets and functions: sets – relations and functions – sequences- Complexity and computability: effectiveness and complexity of algorithms – problems, algorithms and programs – turing machines and un decidability – intractability: P and NP

Total: 45

REFERENCES:

1. Lee E.A. and SeshiaS.A., “Introduction to Embedded Systems - A Cyber-Physical Systems Approach” , 2nd Edition , UC Berkeley, 2017.
2. Peter Marwedel, “Embedded system design – Embedded systems foundations of cyber- physical systems and the Internet of things”, 3rd Edition , Springer Publisher, 2018.
3. http://LeeSeshia.org

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped (Highest Level)**
CO1:	identify the applications and the methods for modeling dynamic behaviors of cyber physical systems	Understanding (K2)
CO2:	explain the concurrent models of computation for the hybrid systems	Understanding (K2)
CO3:	design an embedded system for cyber physical systems	Applying (K3)
CO4:	analyze the invariants and temporal logic models for open and closed systems	Analyzing (K4)
CO5:	analyze the effectiveness and complexity of algorithms	Analyzing (K4)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	3		2		2
CO2			2		
CO3			3	3	2
CO4	3			3	
CO5	3	2		3	1

1 – Slight, 2 – Moderate, 3 – Substantial, BT - Bloom’s Taxonomy

18MWE13 SECURITY ASSESSMENT AND RISK ANALYSIS

L	T	P	Credit
3	0	0	3

Preamble	Security Assessment and Risk Analysis defines the concepts of information security and risk management and explains how they are integral to the management processes used for incident response, disaster recovery and Business Continuity Planning. It also prepares the student to develop and execute plans to enable the organization to recover operations and continue critical business functions in the event of a disaster.
Prerequisites	Computer and Network Security

UNIT – I **9**

Overview of Information Security and Risk Management: Introduction to Information Security - Need for security – Legal, Ethical and Professional issues in Information Security - Security technology - Risk Management

UNIT – II **9**

Contingency Strategies for IR/DR/BC: Contingency Planning and its components - Role of Information Security Policy in Developing Contingency Plans - Data and Application Resumption - Site Resumption Strategies

UNIT – III **9**

Incident Response: Planning - Detection and Decision Making - Organizing and Preparing the CSIRT - Response Strategies - Recovery and Maintenance

UNIT – IV **9**

Disaster Recovery and Business Continuity Planning: Preparation and Implementation - Operation and Maintenance

UNIT – V **9**

Crisis Management: Role and elements of a plan - International standards in IR/DR/BC – Case scenarios for IR/DR/BC

Total: 45

REFERENCES:

1. Whitman, M. E., Mattord, H. J., and Green, A., "Principles of Information Security", 6th Edition, Cengage Learning, 2018.
2. Whitman, M. E., Mattord, H. J., and Green, A., "Principles of incident response and disaster recovery", 2nd Edition, Cengage Learning, 2014.
3. Whitman, M. E., Mattord, H. J., and Green, A., "Hands-on-Information Security Lab Manual", 4th Edition, Cengage Learning, 2014

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped (Highest Level)**
CO1:	outline the concepts of information security and risk management	Understanding (K2)
CO2:	recommend contingency strategies including data backup and recovery and alternate site selection for business resumption planning	Evaluating (K5)
CO3:	inspect the escalation process from incident to disaster in case of security disaster	Analyzing (K4)
CO4:	develop a disaster recovery and business continuity plans for sustained organizational operations	Applying (K3)
CO5:	integrate IR, DR and BC plans into a coherent strategy for crisis management	Creating (K6)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	3	1	3	3	2
CO2	1	1	3	2	2
CO3	2	1	2	3	2
CO4	3	1	3	3	2
CO5	3	1	2	3	2

1 – Slight, 2 – Moderate, 3 – Substantial, BT - Bloom’s Taxonomy

18MWE14 DATABASE SECURITY AND ACCESS CONTROL

L	T	P	Credit
3	0	0	3

Preamble	Provides the fundamentals of database security through user access policies, limitations, RBAC models. Information can be secured based on smart card memory organization and management and access controls
Prerequisites	Nil

UNIT – I		9

Introduction to Access Control: Purpose and fundamentals of access control - brief history - Access Policies and control mechanisms -Policies of Access Control - Models of Access Control and Mechanisms

UNIT – II		9

Discretionary Access Control (DAC): Non- Discretionary Access Control - Mandatory Access Control (MAC) Capabilities and Limitations of Access Control Mechanisms: Access Control List (ACL) and Limitations - Capability List and Limitations

UNIT – III		9

Role Based Access Controls: Role-Based Access Control (RBAC) and Limitations - Core RBAC - Hierarchical RBAC - Statically Constrained RBAC - Dynamically Constrained RBAC - Limitations of RBAC - Comparing RBAC to DAC and MAC Access control policy.

UNIT – IV		9

RBAC Models and Constraints: Biba's integrity model - Clark-Wilson model - Domain type enforcement model - mapping the enterprise view to the system view - Role hierarchies- inheritance schemes - hierarchy structures and inheritance forms, using SoD in real system - Temporal Constraints in RBAC - Integrating RBAC with enterprise IT infrastructures: RBAC for WFMSs, RBAC for UNIX and JAVA environments Case study: Multi line Insurance Company

UNIT – V		9

Smart card Mechanism: Smart Card based Information Security - Smart card operating system fundamentals - design and implantation principles - memory organization and management - file management - atomic operation - quality assurance and testing - smart card life cycle - smart card security - smart card terminals -Recent trends in Database security and access control mechanisms - Case study of Role-Based Access Control (RBAC) systems

Total: 45

REFERENCES:

1. David F. Ferraiolo, D. Richard Kuhn and Ramaswamy Chandramouli, “Role Based Access Control”, 2nd Revised Edition, Artech House, Boston, London, 2007
2. http://www.smartcard.co.uk/tutorials/sct-itsc.pdf : Smart Card Tutorial
3. http://opencarts.org/sachlaptrinh/pdf/10117.pdf

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped (Highest Level)**
CO1:	examine the various access control models	Analyzing (K4)
CO2:	analyse the various access control policies and limitations	Analyzing (K4)
CO3:	recognise the available models of RBAC	Applying (K3)
CO4:	identify the applications of RBAC	Applying (K3)
CO5:	analyse the design of smart card and its mechanisms	Analyzing (K4)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	3			3	2
CO2	3			3	2
CO3		2	3	3	
CO4		2			3
CO5			3	3	

1 – Slight, 2 – Moderate, 3 – Substantial, BT - Bloom’s Taxonomy

18MWE15 PUBLIC KEY INFRASTRUCTURE AND TRUST MANAGEMENT

L	T	P	Credit
3	0	0	3

Preamble	Provide basic knowledge of public key infrastructure and trust management, Which will further enable the students know the basic fundamentals and Gain the knowledge of Secure Public Key Infrastructure Standards and various access control mechanisms.
Prerequisites	Cryptography and Network Security

UNIT – I **9**

PKI: Introduction – services offered by PKI- components of a fully functional PKI : Certification authority, Certificate repository, Certificate revocation, Key backup and recovery, Automatic key update, Key history management, Cross-certification, Support for non-repudiation, Time stamping, Client software

UNIT – II **9**

X.509: PKI architectures – Single CA, Hierarchial PKI, Mesh PKI, Trust Lists, Bridge CAs, PKI standards : X.509: Components of X.509: Tamper evident envelope, Basic certificate contents, certificate extensions.; PGP: Web of Trust.;C) Simple PKI (SPKI) / Simple Distributed Security Infrastructure (SDSI): Representing certificates in terms of S-Expressions- Certificate Chain Discovery - Distinct Advantages of SPKI/SDSI over X.509. PKI application : Smart card integration with PKI's

UNIT – III **9**

Access Control Mechanisms: Discretionary Access Control (DAC) – Mandatory Access Control (MAC) – Role Based Access Control (RBAC) ,Issues : Revocation- Anonymity-Privacy issues

UNIT – IV **9**

Trust Management: Policy based Trust Management System- Social network based Trust Management System- Reputation based Trust Management System (DMRep, EigenRep, P2Prep)- Framework for Trust Establishment

UNIT – V **9**

Trust Models: Introduction - strict v/s loose hierarchy, four corners, distributed. Certificate path processing – path construction and path validation -Trust management challenges, taxonomy framework, architecture, system components, system setting and operations.

Total: 45

REFERENCES:

1. Desmedt, Yvo G. (Ed.), "Secure Public Key Infrastructure Standards", 1st Edition, PGP and Beyond, Springer, 2012
2. Jan Camenisch and Costas Lambrinoudakis, "Public Key Infrastructures, Services and Applications", 1st Revised Selected Articles, 7th European Workshop, Athens, Greece, 2011
3. Carlisle Adams, Steve Lloyd, "Understanding PKI: Concepts, Standards, and Deployment Considerations", 2nd Edition, Addison- Wesley Professional, 2003

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped (Highest Level)**
CO1:	explain the core PKI services such as authentication, integrity, and confidentiality	Understanding (K2)
CO2:	determine appropriate PKI standards for cryptographic applications	Understanding (K2)
CO3:	identify the appropriate access control mechanism in PKI	Applying (K3)
CO4:	describe trust model for Public key certificate management models	Understanding (K2)
CO5:	design certificates using trust models, PKI Considerations and Electronic Legislation	Applying (K3)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	3	2	2		
CO2	2			3	1
CO3	2		3		
CO4			3		
CO5	2		2	3	1

1 – Slight, 2 – Moderate, 3 – Substantial, BT - Bloom’s Taxonomy

18MWE16 INTERNET PROTOCOL AND SECURITY

L	T	P	Credit
3	0	0	3

Preamble	This course on IPv6 Internet Protocol version 6 provides an understanding an next generation Internet Protocol -IPv6, its structure, operation, technical features, addressing, architectures and routing is discussed in detail. They will also comprehend the issues related to Internet infrastructure security, threats, vulnerability and mitigation methods.
Prerequisites	

UNIT – I 9

Introduction: The Disruptive Protocol - Driving IPv6 Growth - A Possible IPv6 Future, IPv4, Patching IPv4 - Network Address Translation (NAT), IPv6 - The Next Generation, IPv6 transition issues.

UNIT – II 9

IPv6 Protocols: The IP Security Protocol (IPsec) - IPv6 Protocol basics - IPv6 Addressing - IPv6 Address Types - IPv6 Address Format - IPv6 Options and Extension Headers - Routing Header - Fragment Header - Hop-by-Hop and Destination Options Headers.

UNIT – III 9

Routing in IPv6: IPv6 Multicast - IPv6 Multicast Address Format - IPv6 Anycast- IPv6 Internet Control message Protocol (ICMPv6) - ICMPv6 Messages- IPv6 Neighbor Discovery - The Neighbor Discovery Protocol - IPv6 Neighbor Discovery Compared with IPv4- IPv6 Routing.

UNIT – IV 9

Vulnerabilities & Threats in IPv6: Introduction to IPv6 Security- IPv6 Protocol Security Vulnerabilities- Layer 3 and Layer 4 Spoofing- IPv6 Internet Security - Large-Scale Internet Threats - Ingress/Egress Filtering - IPv6 Firewalls.

UNIT – V 9

Network Security: Local Network Security - ICMPv6 Layer 2 Vulnerabilities for IPv6 - ICMPv6 Protocol Protection - Network Detection of ICMPv6 Attacks - Network Mitigation Against ICMPv6 Attacks - DHCPv6 Threats and Mitigation- Hardening IPv6 Network Devices - IPv6 Device Management.

Total: 45

REFERENCES:

1. Loshin, Peter, “IPv6: theory, protocol, and practice”, 2nd Edition, Morgan Kaufmann Publications, 2004.
2. Scott Hogg and Eric Vyncke, “IPv6 Security”, 1st Edition, Cisco Press, 2009.
3. William Stallings, “Internet Protocols: Foundation for the Internet, Intranets and Client-Server Computing”,1st Edition, Cambridge University Press, 1996.

COURSE OUTCOMES: On completion of the course, the students will be able to		**BT Mapped** **(Highest Level)**
CO1:	compare the benefits and issues of using IPv4 and IPv6	Understanding (K2)
CO2:	analyze the IPv6 protocol and its address format	Analyzing (K4)
CO3:	build the network route discovery using IPv6 and ICMPv6	Applying (K3)
CO4:	identify the various vulnerabilities and threats in IPv6	Applying (K3)
CO5:	analyze the network security attacks and mitigation using IPv6	Analyzing (K4)

Mapping of COs with POs

COs/POs	PO1	PO2	PO3	PO4	PO5
CO1	2	2	2		3
CO2	3	3	1		2
CO3	2	2	3	1	
CO4	2		1	2	3
CO5	1		1	3	3

1 – Slight, 2 – Moderate,   3 – Substantial, BT - Bloom’s Taxonomy