R25-COURSE STRUCTURE
(M.TECH. CYBER SECURITY)

I SEMESTER

S.No.	Course code	Course Title	Contact hours/week			Credits	Scheme of Valuation		
			L	T	P		CIE	SEE	Total
Theory Courses									
1	D2512601	Mathematical Foundations For Security	3	1	0	4	40	60	100
2	D2512602	Advanced Data Structures	3	1	0	4	40	60	100
3	D2512603	Principles Of Cyber Security	3	1	0	4	40	60	100
4	**PROGRAMELECTIVE–I**		3	0	0	3	40	60	100
5	**PROGRAMELECTIVE–II**		3	0	0	3	40	60	100
Laboratory Courses									
6	D2512690	Advanced Data Structures Lab	0	1	2	2	40	60	100
7	D2512691	Cyber Security Lab	0	1	2	2	40	60	100
8	D2510080	Seminar-I	0	0	2	1	100	-	100
Total			**15**	**5**	**6**	**23**	380	420	800

List of Professional Elective Courses in I Semester (Electives – I & II)

Course Code	Course Title
D25126A0	Operating System Security
D25126A1	Firewall and VPN Security
D25126A2	Intrusion Detection
D25126B0	Database and Web Application Security
D25126B1	Secure Software Design and Development
D25126B2	Wireless Network Security

@ Minimum 2/3 themes per elective

II SEMESTER

S.No.	Course code	Course Title	Contact hours/week			Credits	Scheme of Valuation		
			L	T	P		CIE	SEE	Total
Theory Courses									
1	D2522601	Vulnerability Assessment and Penetration Testing	3	1	0	4	40	60	100
2	D2522602	Malware Analysis & Reverse Engineering	3	1	0	4	40	60	100
3	D2522603	Cyber Crime Investigation & Digital Forensics	3	1	0	4	40	60	100
4	**Program Elective – III**		3	0	0	3	40	60	100
5	**Program Elective – IV**		3	0	0	3	40	60	100
Laboratory Courses									
6	D2522690	Vulnerability Assessment and Penetration Testing Lab	0	1	2	2	40	60	100
7	D2522691	Digital Forensics Lab	0	1	2	2	40	60	100
8	D2520080	Seminar-II	0	0	2	1	100	-	100
Total			**15**	**5**	**6**	**23**	**380**	**420**	**800**

List of Professional Elective Courses in II Semester (Electives III & IV)

Course Code	Course Title
D25226A0	Cloud and IoT Security
D25226A1	AI for Cyber security
D25226A2	Data Privacy
D25226B0	Principles of Secure Coding
D25226B1	Security Assessment and Risk Analysis
D25226B2	Biometric Security

@ Minimum 2/3 themes per elective

III SEMESTER

S.No	Course code	Course Title	Contact hours/week			Credits	Scheme of Valuation		
			L	T	P		CIE	SEE	Total
Theory Courses									
1	D2530001 / M	Research Methodology and IPR / Swayam *12-week MOOC course – RM&IPR*	3	0	0	3	40	60	100
2	D253000S	Summer Internship/ Industrial Training (8-10 weeks)*	-	-	-	3	100	-	100
3	D25300CV	Comprehensive Viva#	-	-	-	2	100		100
4	D253000P	Dissertation Part – A$	-	-	20	10	100		100
Total			**3**	**0**	**20**	**18**	340	60	400

***Student attended during summer / year break and assessment will be done in 3rd Sem. #**
Comprehensive viva can be conducted courses completed upto second sem.
$ Dissertation – Part A, internal assessment

IVSEMESTER

S.No	Course code	Course Title	Contact hours/week			Credits	Scheme of Valuation		
			L	T	P		CIE	SEE	Total
1	D254000P	Dissertation Part – B%	-	-	32	16	-	100	100
Total			0	0	32	16	0	100	100

% External Assessment

Total Credits: 23+23+18+16= 80

I Semester	D2512601-MATHEMATICAL FOUNDATIONS FOR SECURITY	L	T	P	C
		3	1	0	4

Course Objectives:

1. To understand the mathematical fundamentals in probabilistic and statistical concepts
2. To develop the understanding of the mathematical and logical basis of various modern techniques in information technology like machine learning, programming language design, and concurrency.
3. To study various Graph Theory problems.

Course Outcomes: On completion of this course, the student will be able to:

CO	Course Outcome	Bloom's Level
CO1	Use concepts of discrete and continuous probability, including PDF, CDF, expectation, and Markov chains, to solve computational problems.	L3 – Apply
CO2	Implement sampling distributions and statistical inference techniques to solve data mining and machine learning problems.	L3 – Apply
CO3	Employ statistical analysis and model evaluation techniques to solve computational problems.	L3 – Apply
CO4	Use graph theory and combinatorial techniques to model and solve computer science problems.	L3 – Apply
CO5	Utilize number theoretic methods, including modular arithmetic and modular exponentiation, to solve cryptographic problems.	L3 – Apply

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	H		M	H		
CO2	H		H	H	M	
CO3	H		H	H	M	
CO4			H	H	M	
CO5			M	H	H	M

UNIT	CONTENTS
UNIT -1	Density, and cumulative distribution functions, Expected value, conditional expectation, Applications of the univariate and multivariate Central Limit Theorem, Probabilistic inequalities, Markov chains.
UNIT –2	Random samples, sampling distributions of estimators, and Maximum Likelihood

UNIT – 3	Statistical inference, Introduction to multivariate statistical models: classification problems, principal component analysis, The problem of over fitting model assessment
UNIT – 4	Graph Theory: Isomorphism, Planar graphs, graph coloring, Hamilton circuits and Euler cycles. Permutations and Combinations with and without repetition. Specialized techniques to solve combinatorial enumeration problems
UNIT – 5	Number Theory: Elementary number theory, unique factorization, Euler's function, modular arithmetic, Fermat's little theorem, Chinese remainder theorem, modular exponentiation,RSA public key encryption

Text Books:

1. John Vince, Foundation Mathematics for Computer Science, Springer, 2015.
2. K. Trivedi, Probability and Statistics with Reliability, Queuing, and Computer Science Applications, Wiley, 2001.

Reference Books:

1. M. Mitzenmacher and E. Upfal, Probability and Computing: Randomized Algorithms and Probabilistic Analysis, 2005.
2. Alan Tucker, Applied Combinatorics, Wiley, 2012.

I Semester	D2512602-ADVANCED DATA STRUCTURES	L	T	P	C
		3	1	0	4

Course Objectives: The course is taught with the objectives of enabling the student to:

- Understand the ADT/libraries and choose appropriate data structures to design algorithms for a specific problem.
- Understand the necessary mathematical abstraction to solve problems.
- To familiarize students with advanced problem-solving paradigms and data structure used to solve algorithmic problems.
- Analysis of efficiency and proof of correctness

Course Outcomes: On completion of this course, the student will be able to:

CO	Course Outcome	Bloom's Level
CO1	Use the principles of dictionaries, abstract data types, and hashing techniques, including hash function design and collision resolution methods, to solve data organization problems.	L3 – Apply
CO2	Implement skip list operations such as search and update using probabilistic and deterministic approaches for efficient data organization.	L3 – Apply
CO3	Use appropriate tree data structures and their operations to solve computational problems involving hierarchical data organization.	L3 – Apply
CO4	Employ text processing algorithms, including pattern matching techniques, tries, Huffman coding, and dynamic programming approaches, to solve text processing problems.	L3 – Apply
CO5	Utilize computational geometry techniques, including range searching, priority search trees, quad trees, and k-D trees, to solve geometric searching problems.	L3 – Apply

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	H		M	H		
CO2	H		H	H		
CO3	H		H	H		
CO4	H		H	H		
CO5	H		H	H		

UNIT	CONTENTS	Contact
UNIT – 1	**Dictionaries:** Definition, Dictionary Abstract Data Type, Implementation of Dictionaries. Hashing: Review of Hashing, Hash Function, Collision Resolution Techniques in Hashing, Separate Chaining, Open Addressing, Linear Probing, Quadratic Probing, Double Hashing, Rehashing, Extendible Hashing.	12
UNIT – 2	**Skip Lists:** Need for Randomizing Data Structures and Algorithms, Search and Update Operations on Skip Lists, Probabilistic Analysis of Skip Lists, Deterministic Skip Lists.	12
UNIT – 3	**Trees:** Binary Search Trees, AVL Trees, Red Black Trees, 2-3 Trees, B-Trees, Splay Trees	12
UNIT – 4	**Text Processing:** String Operations, Brute-Force Pattern Matching, The Boyer-Moore Algorithm. The Knuth-Morris-Pratt Algorithm, Standard Tries, Compressed Tries, Suffix Tries, The Huffman Coding Algorithm, The Longest Common Subsequence Problem (LCS), Applying Dynamic Programming to the LCS Problem.	12
UNIT – 5	**Computational Geometry:** One-Dimensional Range Searching, Two-Dimensional Range Searching, constructing a Priority Search Tree, Searching a Priority Search Tree, Priority Range Trees, Quad trees, k-D Trees.	12
	Total	60

Text Books:

1. Data Structures: A Pseudo-code Approach, 2/e, Richard F.Gilberg, BehrouzA.Forouzon, Cengage
2. Data Structures, Algorithms and Applications in java, 2/e, SartajSahni, University Press

Reference Books:

1. Mark Allen Weiss, Data Structures and Algorithm Analysis in C++, 2nd Edition, Pearson, 2004.
2. M T Goodrich, Roberto Tamassia, Algorithm Design, John Wiley, 2002.

I Semester	D2512603- PRINCIPLES OF CYBER SECURITY	L	T	P	C
		3	1	0	4

Course Objectives:

- To learn threats and risks with in context of the cyber security architecture.
- Student should learn and Identify security tools and hardening techniques.
- To learn types of incidents including categories, responses and timelines for response.

Course Outcomes: On completion of this course, the student will be able to:

CO	Course Outcome	Bloom's Level
CO1	Explain cyber security architecture principles and their role in protecting information systems.	**L2 – Understand**
CO2	Analyze risk management processes and practices to identify and assess cyber security risks.	**L4 – Analyze**
CO3	Implement appropriate response techniques to address cyber security incidents.	**L3 – Apply**
CO4	Analyze system and application security threats and vulnerabilities to determine potential security risks.	**L4 – Analyze**
CO5	Implement security tools and hardening techniques to strengthen system security.	**L3 – Apply**

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		M		H	M
CO2	H		M		H	H
CO3	M		M	H	H	
CO4	M		M	H	H	M
CO5	M		M		M	M

UNIT	CONTENTS	Contact Hours
UNIT– 1	**Introduction to Cyber Security**- Cyber security objectives, cyber security roles, differences between information security and cyber security, cyber security principles (confidentiality, integrity, and availability), authentication, and non-repudiation.	12
UNIT– 2	**Information Security (IS) within Lifecycle**-Management-Lifecycle management landscape, Security architecture processes, Security architecture tools, Intermediate life cycle management concepts, Risks &Vulnerabilities-Basics of risk management, Operational threat environments, Classes of attacks.	12
UNIT– 3	**Incident Response and Operational Security Protection**- Incident categories, Incident response Incident recovery, and Operational security protection: Digital and data assets, Ports and protocols, Protection technologies, Identity and access	12

	Management, configuration management.	
UNIT– 4	**Threat Detection and Evaluation (DE):** Monitoring- Vulnerability Management, Security Logs and Alerts, Monitoring Tools and Appliances. Analysis Network traffic Analysis, packet capture and analysis	12
UNIT– 5	**Introduction to Backdoor Systems and Security**- Introduction to metasploit, Backdoor, demilitarized zone(DMZ),Digital Signature, Brief study on Harding of operating system.	12
	Total	**60**

Text Books:

1. NASSCOM: SecurityAnalyst StudentHandBookDec2015.
2. Information Security Management Principles **Updated Edition** byDavid Alexander, Amanda Finch, David Sutton, Published by BCS, June 2013.

Reference Books:

1. CSX- cyber security fundamentals 2 nd edition, Published by ISACA, Cyber security, Network Security, Data Governance Security.

Semester-I	D25126A0- OPERATING SYSTEM SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

- Students will learn and apply basic concepts and methodologies of System Administration and Security by building from the ground up a miniature corporate network.
- To know some basic security measures to take in system administration.
- To prepare for possible disasters, including an understanding of backup and restoration of file systems.

Course Outcomes:

On completion of this course, the student will be able to:

CO	Course Outcome Statement	Bloom's Level
CO1	Explain the overview and fundamental concepts of operating systems.	L2 – Understand
CO2	Demonstrate operating system protection mechanisms to safeguard system resources.	L3 – Apply
CO3	Analyze operating system security concepts covering threats, attacks, encryption, authentication, and system protection.	L4 – Analyze
CO4	Implement system administration practices for server security, monitoring, auditing, configuration management, and vulnerability assessment.	L3 – Apply
CO5	Configure Linux networking and security techniques across services, firewalls, IDS/SSH, and system coexistence scenarios.	L3 – Apply

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		M			
CO2	M		M	H	H	
CO3	M		M	H	H	M
CO4	H		M	H	H	M
CO5	M		M	H	H	

UNIT	CONTENTS	Contact Hours
UNIT – 1	Overview of Operating Systems-Introduction, Computer system organization and architecture, Operating system structure and operations, Process Management, Memory Management, file systems management Protection and security, Scheduling Algorithms, Inter-process Communication(TB1)	12
UNIT – 2	Operating Systems Protection: Protection Goals, Protection Threats, Access Control Matrix, Access Control Lists(ACL's), Capability Lists(C-lists), Protection systems, Lampson's access matrix, mandatory protection systems, Reference monitor, Secure operating system definition(TB2)	12
UNIT – 3	Operating System Security-Security Goals, Security Threats, Security Attacks- Trojan Horses, Viruses and Worms, Buffer Overflow attacks and Techniques, Formal Aspects of Security, Encryption- Attacks on Cryptographic Systems, Encryption Techniques, Authentication and Password Security, Intrusion detection, malware defences, UNIX and Windows security(TB2)	12
UNIT – 4	System Administration: Security Basics, Securing the Server Itself, Maintenance and Recovery, Monitoring and Audit, Introduction to Linux Systems, Configuration Management, Log Auditing and Vulnerability Assessment.(TB3)	12
UNIT – 5	Linux Networking: Networking Technologies: DHCP, DNS, NFS/ISCSI, SMTP, SNMP, LAMP, Firewall/IDS/SSH, Securing Linux. Case Studies: Security and Protection-MULTICS, UNIX, LINUX and Windows, Windows and Linux Coexisting.(TB4)	12
	Total	60

Text Books:

1. Operating System Concepts, 9th Edition, Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, Wiley Publication, 2008
2. Operating Systems: A Concept-Based Approach, 3rd Edition, Dhananjay M. Dhamdhere, McGraw- Hill, 2015
3. Windows Server 2003 Security, A Technical Reference, Roberta Bragg, Addisson-Wesley
4. Linux Administration Handbook, Second Edition, Evi Nemeth, Garth Snyder, Trent R. Hein. Prentice Hall

Reference Books:

1. An Introduction to Operating Systems: Concepts and practice, 4th Edition, Promod Chandra P Bhat, Prentice Hall of India, 2014.
2. Operating System: Internals and Design Principles, 7th Edition, William Stalling, Prentice Hall, 2014Linux System Administration, Tom Adelstein and Bill Lubanovic, First Edition, O'Reilly Media, Inc.

I Semester	D25126A1- FIREWALL AND VPN SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

- Identify and assess current and anticipated security risks and vulnerabilities
- Develop a network security plan and policies
- Establish a VPN to allow IPSec remote access traffic
- Monitor, evaluate and test security conditions and environment
- Develop critical situation contingency plans and disaster recovery plan
- Implement/test contingency and backup plans and coordinate with stakeholders
- Monitor, report and resolve security problems

Course Outcomes: On completion of this course, the student will be able to:

CO	Course Outcome Statement	Bloom's Level
CO1	Explain the fundamentals of firewalls, their types, and deployment mechanisms.	L2 – Understand
CO2	Implement VPN concepts, cryptographic techniques, and authorization mechanisms to establish secure remote connections.	L3 – Apply
CO3	Examine firewall rules, logs, alerts, and intrusion detection mechanisms to identify security threats.	L4 – Analyze
CO4	Examine the design and operation of Industrial Control Systems, including SCADA, DCS, PLC, and ICS.	L4 – Analyze
CO5	Assess SCADA protocols and vulnerabilities in industrial communication systems to determine potential security risks.	L5 – Evaluate

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		M	H	H	
CO2	H		H	H	H	M
CO3	H		H	H	H	H
CO4	M		H	H	H	M
CO5	M		H	H	H	M

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	Contact Hours
UNIT – 1	Firewall Fundamentals: Introduction, Types of Firewalls, Ingress and Egress Filtering, Types of Filtering, Network Address Translation (NAT), Application Proxy, Circuit Proxy, Content Filtering, Software versus Hardware Firewalls, IPv4 versus IPv6 Firewalls, Dual-Homed and Triple-Homed Firewalls, Placement of Firewalls.	12
UNIT – 2	VPN Fundamentals: VPN Deployment Models and Architecture, Edge Router, Corporate Firewall, VPN Appliance, Remote Access, Site-to-Site, Host-to-Host, Extranet Access, Tunnel versus Transport Mode, The Relationship Between Encryption and VPNs, Establishing VPN Connections with Cryptography, Digital Certificates, VPN Authorization.	12
UNIT – 3	Exploring the Depths of Firewalls: Firewall Rules, Authentication and Authorization, Monitoring and Logging, Understanding and Interpreting Firewall Logs and Alerts, Intrusion Detection, Limitations of Firewalls, Downside of Encryption with Firewalls, Firewall Enhancements, and Management Interfaces	12
UNIT – 4	Overview of Industrial Control Systems: Overview of SCADA, DCS, and PLCs, ICS Operation, Key ICS Components, Control Components, Network Components, SCADA Systems, Distributed Control Systems, Programmable Logic Controllers, Industrial Sectors and Their Interdependencies.	12
UNIT – 5	SCADA Protocols: Modbus RTU, Modbus TCP/IP, DNP3, DNP3 TCP/IP, OPC, DA/HAD, SCADA protocol fuzzing, Finding Vulnerabilities in HMI: software- Buffer Overflows, Shell code. Previous attacks Analysis- Stuxnet, Duqu.	12
	Total	60

Text Books:

1. Michael Stewart “Network Security, Firewalls, and VPNs” Jones & Bartlett Learning September 2010.
2. T. Macaulay and B. L. Singer, Cyber security for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS, Auerbach Publications, 2011.
3. J. Lopez, R. Setola, and S. Wolthusen, Critical Infrastructure Protection Information Infrastructure Models, Analysis, and Defense, Springer-Verlag Berlin Heidelberg, 2012.

Reference Books:

1. J. Lopez, R. Setola, and S. Wolthusen, Critical Infrastructure Protection Information Infrastructure Models, Analysis, and Defense, Springer-Verlag Berlin Heidelberg, 2012.
2. Robert Radvanovsky and Jacob Brodsky, editors. Handbook of SCADA/Control Systems Security. CRC Press, 2013.
3. A.W. Colombo, T. Bangemann, S. Karnouskos, S. Delsing, P. Stluka, R. Harrison, et al. Industrial cloud-based cyber-physical systems Springer International Publishing, 2014.D. Bailey, Practical SC

I Semester	D25126A2- INTRUSION DETECTION	L	T	P	C
		3	0	0	3

Course Objectives:

The outcome of this course is to:

- Compare alternative tools and approaches for Intrusion Detection through quantitative analysis to determine the best tool or approach to reduce risk from intrusion.
- Identify and describe the parts of all intrusion detection systems and characterize new and emerging IDS technologies according to the basic capabilities all intrusion detection systems share.

Course Outcomes: On completion of this course, the student will be able to:

CO	Course Outcome Statement	Bloom's Level
CO1	Explain the fundamentals and historical evolution of Intrusion Detection Systems to recognize common pitfalls in their design and evaluation.	L2 – Understand
CO2	Implement Intrusion Detection tools and techniques to assess and improve enterprise security.	L3 – Apply
CO3	Describe the classification of Intrusion Detection Systems and the principles of signature-based and anomaly-based detection techniques.	L2 – Understand
CO4	Configure Snort rules, installation procedures, and alert mechanisms for effective intrusion detection.	L3 – Apply
CO5	Employ advanced IDS models, malware detection methods, and security strategies to address insider threats and emerging challenges.	L3 – Apply

Course Articulation Matrix:

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	H		H	M	H	M
CO2	H		H	H	H	H
CO3	M		H	H	H	H
CO4	M		H	H	H	H
CO5	H		H	H	H	H

UNIT	CONTENTS	Contact Hours
UNIT – 1	The state of threats against computers and networked Systems- Overview of computer security solutions and why they Fail- Vulnerability assessment, firewalls, VPN's–Overview of Intrusion Detection and Intrusion Prevention- Network and Host-based IDS.	12

UNIT – 2	Classes of attacks – Network layer: scans, denial of service, penetration – Application layer**:** software exploits, code Injection-Human layer**:** identity theft, root access-Classes of attackers-Kids/hackers/sop Hesitated groups-Automated**:** Drones, Worms,Viruses.	12
UNIT – 3	A General IDS model and taxonomy, Signature-based Solutions, Snort, Snort rules, Evaluation of IDS, Cost sensitive IDS Anomaly Detection Systems and Algorithms-Network Behaviour Based Anomaly Detectors (rate based)-Host-based Anomaly Detectors Software Vulnerabilities-State transition, Immunology, Payload Anomaly Detection.	12
UNIT – 4	Attack trees and Correlation of Alerts-Autopsy of Worms and Botnets-Malware Detection-Obfuscation, Polymorphism-Document vectors. Email/IM security Issues-Viruses/Spam-From signatures to thumbprints to zero day. Detection-Insider Threat Issues-Taxonomy Masquerade and Impersonation-Traitors, Decoys and Deception-Future**:** Collaborative Security.	12
UNIT – 5	Introduction to Snort, Snort Installation Scenarios, Installing Snort, Running Snort on Multiple Network Interfaces, Snort Command Line Options. Step-By-Step Procedure to Compile and Install Snort Location of Snort Files, Snort Modes Snort Alert Modes.	12
	Total	60

Text Books:

1. Network Security Essentials: Applications and Standards – by William Stallings.
2. Intrusion Detection and Prevention Systems – by Carl Endorf, Eugene Schultz, Jim Mellander.

References:

1. Szor, P. (2010). The Art of Computer Virus Research and Defense, United States: Symantec Press.
2. Jakobsson, M., and Ramzan, Z. (2008). Crimeware, Understanding New Attacks and Defenses,United States: Symantec Press.
3. Research Articles from SCI & Scopus indexed Journals.

I Semester	D25126B0- DATABASE AND WEB APPLICATION SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

- To acquire knowledge on standard algorithms used to provide confidentiality, integrity and authenticity.
- To design security applications in the field of Information technology.
- To understand the fundamentals of database design, DB security and SQL extensions to security.
- To learn the basic concepts of Penetration testing.

Course Outcomes: On completion of this course, the student will be able to:

CO	Course Outcome	Bloom's Level
CO1	Analyze threats, vulnerabilities, and breaches to identify security requirements for database systems.	L4 – Analyze
CO2	Explain the relational model, concurrency control, and SQL security extensions.	L2-Understand
CO3	Implement web application and browser security principles to address common security threats.	L3 – Apply
CO4	Implement mobile device and application security mechanisms in real-time applications.	L3 – Apply
CO5	Execute penetration testing workflows to identify vulnerabilities in real-world scenarios.	L3 – Apply

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		H	H	H	M
CO2	M		H	H	H	
CO3	M		H	H	H	M
CO4	H		H	H	H	M
CO5	H		H	H	H	H

UNIT-I **Database security** - Introduction includes threats, vulnerabilities and breaches, Basics of database design, DB security, concepts, approaches and challenges, types of access controls, Oracle VPD. **Discretionary and Mandatory access control** - Principles, applications and poly instantiation, Database inference problem, types of inference attacks, distributed database, security levels, **SQL-injection:** types and advanced concepts
UNIT -II **Relational Data Model -** Security in relational data model, concurrency controls and locking, SQL extensions to security (oracle as an example), System R concepts, Context and control-based access control, Hippocratic databases, Database watermarking, Database intrusion, secure data outsourcing.
UNIT -III **Web application security -** Basic principles and concepts, Authentication, Authorization, Browser security principles; XSS and CSRF, same origin policies, File security principles, Secure development and deployment methodologies, Web DB principles, OWASP – Top 10 -Detailed treatment, IoT security.
UNIT - IV **Mobile device security**-Introduction, attack vector and models, hardware centric security aspects, SMS / MMS vulnerabilities, software centric security aspects, mobile web browser security. **Application security:** Concepts, CIA Triad, Hexad, types of cyber-attacks, Introduction to software development vulnerabilities, code analyzers– Static and dynamic analyzers.
UNIT -V **Penetration testing -** Principles and concepts, PT work flows and examples, blind tests, ethical hacking techniques, synthetic transactions, interface testing and fuzzing, SDLC phases and security mandates.

Text Books:

1. Bryan and Vincent, "Web Application Security, A Beginners Guide ", McGraw-Hill, 2011
2. Alfred Basta, Melissa Zgola, "Database Security", Course Technology, 2012.

Reference Books:

1. Michael Gertz and Sushil Jajodia, "Handbook of Database Security—Applications and Trends", Springer, 2008.
2. Bhavani Thuraisingham, "Database and Applications Security", Integrating Information Security and Data Management, Auerbach Publications, 2005.

I Semester	D25126B1- SECURE SOFTWARE DESIGN AND DEVELOPMENT	L	T	P	C
		3	0	0	3

Course Objectives:

- To fix software flaws and bugs in various software.
- To make students aware of various issues like weak random number generation, information leakage, poor usability, and weak or no encryption on data traffic.
- Techniques for successfully implementing and supporting network services on an enterprise scale and heterogeneous systems environment.
- Methodologies and tools to design and develop secure software containing minimum vulnerabilities and flaws.

Course Outcomes: On completion of this course, the student will be able to:

CO#	Course Outcome	Knowledge Level(K)#
CO1	Demonstrate various software vulnerabilities and software security design concepts.	L2-Understand
CO2	Design distributed N-tier enterprise applications by identifying appropriate presentation, business, and data layer technologies.	L3-Apply
CO3	Design and manage enterprise server infrastructure and network services ensuring reliability and availability.	L3-Apply
CO4	Apply enterprise networking knowledge to manage and troubleshoot multi-service networks efficiently.	L3-Apply
CO5	Describe case studies on DNS server operations, DHCP configuration and SQL injection attacks.	L3-Apply

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		H	H	H	M
CO2	M		H	H	H	
CO3	M		H	H	H	M
CO4	H		H	H	H	M
CO5	H		H	H	H	H

UNIT-I

Secure Software Design-Identify software vulnerabilities and perform software security analysis, Master security programming practices, Master fundamental software security design concepts, Perform security testing and quality assurance.

UNIT -II

Enterprise Application Development- Describe the nature and scope of enterprise software applications, Design distributed N-tier software application, Research technologies available for the presentation, business and data tiers of an enterprise software application, Design and build a database using an enterprise database system, Develop components at the different tiers in an enterprise system, Design and develop a multi-tier solution to a problem using technologies used in enterprise system, Present software solution.

UNIT -III

Enterprise Systems Administration-Design, implement and maintain a directory-based server infrastructure in a heterogeneous systems environment, monitor server resource utilization for system reliability and availability, Install and administer network services (DNS/DHCP/Terminal Services/Clustering/Web/Email).

UNIT -IV

Obtain the ability to manage and troubleshoot a network running multiple services, understand the requirements of an enterprise network and how to go about managing them.

Unit-V

Handle insecure exceptions and command/SQL injection, Defend web and mobile applications against attackers, software containing minimum vulnerabilities and flaws, Case study of DNS server, DHCP configuration and SQL injection attack.

Text Books:

1. Theodor Richardson, Charles N Thies, Secure Software Design, Jones & Bartlett
2. Kenneth R. van Wyk, Mark G. Graff, Dan S. Peters, Diana L. Burley, Enterprise Software Security, Addison Wesley.

I Semester	D25126B2- WIRELESS NETWORK SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

- To understand the concepts of network security threats, classify the threats and develop a security model to prevent, detect and recover from the attacks.
- Student should learn and Develop SSL or Firewall based solutions against security threats, employ access control techniques to the existing computer platforms such as UNIX and Windows NT.
- To learn and understand wireless technologies and apply real-time applications

Course Outcomes: On completion of this course, the student will be able to:

CO	Course Outcome	Bloom's Level
CO1	Explain the evolution of wireless technologies and identify security risks associated with Rogue Network Access Points.	L2 – Understand
CO2	Implement wireless LAN security protocols and SSL/TLS mechanisms to establish secure wireless communication.	L3 – Apply
CO3	Analyze FDMA and GSM security mechanisms and evaluate the underlying algorithms for wireless communication security.	L4 – Analyze
CO4	Analyze current and emerging wireless technologies and standards with respect to their security features and applications.	L4 – Analyze
CO5	Implement basic Bluetooth security specifications and mechanisms for secure wireless communication.	L3 – Apply

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		H	M	H	M
CO2	H		H	H	H	H
CO3	M		H	H	H	M
CO4	M		H	M	H	
CO5	M		H	M	H	M

UNIT – I

Introduction to Wireless: History of Wireless Technologies, History of Wireless Security, State of the Wireless Security Industry, **Wireless Threats:** Uncontrolled Terrain, Communications Jamming, DoS Jamming, Injections and Modifications of Data, Man-in-the-Middle (MITM) Attack, Rogue Client, Rogue Network Access Points, Attacker Equipment, Covert Wireless Channels, Roaming Issues, Cryptographic Threats

UNIT – II

Introduction to Wireless Security Protocols and Cryptography: Recovery the FUD, OSI Model, OSI Simplified, Internet Model, Wireless LAN Security Protocols, Cryptography, SSL/TLS, Secure Shell Protocols, Terminal Access and File Transfer, Port Forwarding a Word of Caution, Man-in-the-Middle of SSL/TLS and SSH, WTLS, WEP,802.1x, IP Security. **Security Considerations to Wireless Devices:** Wireless Device Security Issues, Physical Security, Information Leakage, Device Security Features, Application Security, Detailed Device Analysis, Laptops, Personal Digital Assistants (PDAS), Wireless Infrastructure

UNIT – III

Wireless Technologies and Applications: Introduction to Cellular Networks- FDMA, TDMA, CDMA, Spread Spectrum Primer, Analogy, TDMA Vs CDMA, PDC, Security Threats, GSM Security, GSM Algorithm Analysis. **Introduction to Wireless Data Networks:** Cellular Digital Packet Data (CDPD), CDPD Architecture, CDPD Security, Mobitex-Mobitex Architecture, Mobitex Security Architecture, General Packet Radio Service (GPRS)- GPRS Architecture, Security Issues, Introduction to the Wireless Application Protocol (WAP)- WAP Device, Gateway, Security Model

UNIT – IV

Wireless Standards and Technologies: Current and Future Technologies- Infrared, Radio, Spread Spectrum, OFDM, Current and Future Standards- IEEE 802, 802.11, The ABC's of 802.11, 802.11b, 802.11a, 802.11g, 802.11j, 802.11h and 5GPP, 802.11e, 802.11i, 802.11f, IEEE 802.15, IEEE 802.16, IEEE 802.1x, ETSI, Home RF, Ultra wideband Radio (UWB).

Wireless Deployment Strategies: Implementing Wireless LAN's- Security Considerations Common Wireless Network Applications, Enterprise Campus Designs, Wireless IST Design, Retail and Manufacturing, Design, Small Office/Home Office Design (SOHO)

UNIT – V

Bluetooth Security: Basic specifications, Pico-nets, Bluetooth security architecture, Scatter-nets, Security at the baseband layer and link layer, Frequency hopping, Security manager, Authentication, Encryption, And Threats to Bluetooth security

Text Books:

1. Merritt Maxim and David Pollino, "Wireless Security", Osborne/McGraw Hill, New Delhi, 2005
2. Nichols and Lekka, "Wireless Security-Models, Threats and Solutions", Tata McGraw – Hill, New Delhi, 2006.
3. Charles P. Fleeger, "Security in Computing", Prentice Hall, New Delhi, 2009

Reference Books:

1. BehrouzA.Forouzan, —Cryptography & Network Security, Tata McGraw Hill, India, New Delhi, 2009.
2. William Stallings, —Cryptography and Network Security, Prentice Hall, New Delhi, 2006.

I Semester	D2512690- ADVANCED DATA STRUCTURES LAB	L	T	P	C
		0	1	2	2

Course Objectives:

From the course the student will learn

- Knowing about oops concepts for a specific problem.
- Various advanced data structures concepts like arrays, stacks, queues, linked lists, graphs and trees.

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (L)
CO1	Implement fundamental data structures such as multi stacks, deques, and circular queues to manage and organize data efficiently.	L3-Apply
CO2	Apply recursive and non-recursive operations on Binary Search Trees and implement graph traversal algorithms like BFS and DFS.	L3-Apply
CO3	Analyze and implement various sorting algorithms such as Merge Sort, Heap Sort, and Quick Sort, and compare their performance.	L4-Analyze

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		H	H		
CO2	M		H	H		
CO3	H		H	H		

Experiment	CONTENTS
Experiment 1:	Implement Multi stacks.
Experiment 2:	Implement Double Ended Queue (Dequeues) & Circular Queues.
Experiment 3:	Implement various Recursive operations on Binary Search Tree.
Experiment 4:	Implement various non-recursive operations on Binary Search Tree.
Experiment 5:	Implement BFS for a Graph
Experiment 6:	Implement DFS for a Graph.
Experiment 7:	Implement Merge & Heap Sort of given elements.
Experiment 8:	Implement Quick Sort of given elements.
Experiment 9:	Implement various operations on AVL trees.
Experiment 10:	Implement B: Tree operations.
Experiment 11:	Implementation of Binary trees and Traversals (DFT, BFT)
Experiment 12:	Implement Krushkal's algorithm to generate a min-cost spanning tree.
Experiment 13:	Implement Prim's algorithm to generate a min-cost spanning tree.
Experiment 14:	Implement functions of Dictionary using Hashing.

I Semester	D2512691- CYBER SECURITY LAB	L	T	P	C
		0	1	2	2

Course Objectives:

- Student to get the knowledge about audit and information security management, which makes the student to get the real world experience.
- To learn and implement Data leakage in a website database

Course Outcomes: On completion of this course, the student will be able to:

		Blooms Levels
CO1	Apply audit security policies in a Windows environment and implement the design of a Demilitarized Zone (DMZ) in network environments	L3-Apply
CO2	Apply mitigation techniques for cyber security threats including resource-harvesting attacks, Trojans, data leakage, and patch management	L3-Apply
CO3	Analyze and evaluate cyber security tools and techniques such as Metasploit, access control lists (ACLs), content filtering, audit policies, and event log analysis for securing systems and networks	L4-Analyze

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	3		3	3	3	3
CO2	2		3	3	3	3
CO3	2		3	3	3	3

Exercise	CONTENTS
Exercise–1:	Implement and analyze audit security policies in a Windows environment.
Exercise–2:	Create a demilitarized zone (DMZ) in a network environment for information security.
Exercise–3:	Implement a resource-harvesting attack in a lab setup and demonstrate mitigation techniques.
Exercise–4:	Implement a Windows patch management policy.
Exercise–5:	Study the behavior of Trojans and implement mitigation strategies.
Exercise–6:	Set up a Metasploit environment and use it to launch and analyze an attack in a controlled lab.
Exercise–7:	Create access control lists (ACLs) and configure content filtering to limit network traffic.
Exercise–8:	Analyze data leakage in a website database and implement preventive measures.
Exercise–9:	Implement password policies and verify their enforcement.
Exercise–10:	Implement patch management using the MBSA tool on a Windows machine.
Exercise–11:	Configure and analyze audit policy management for users and computers, including log analysis.
Exercise–12:	Implement a media handling policy and perform event log analysis.
Exercise–13:	Install a Trojan in a controlled lab environment and study its different options and behaviors.
Exercise–14:	Conduct a network DoS attack in a controlled environment, demonstrate bandwidth utilization, and implement preventive steps.

II Semester	D2522601- VULNERABILITYASSESSMENT & PENETRATION TESTING	L	T	P	C
		3	1	0	4

Course Objectives:

- To identify security vulnerabilities and weaknesses in the target applications.
- To identify how security controls can be improved to prevent hackers gaining access to operating systems and networked environments.
- To test and exploit systems using various tools.
- To understand the impact of hacking in real time machines.

Course Outcomes: On completion of this course, the student will be able to:

CO	Course Outcome	Knowledge Level (L)
CO1	Explain the phases of penetration testing and their role in identifying security vulnerabilities in systems and networks.	L2
CO2	Explain information-gathering methodologies used in penetration testing.	L2
CO3	Apply system hacking techniques to identify and assess security vulnerabilities in controlled environments.	L3
CO4	Explain techniques used to bypass WLAN authentication mechanisms.	L2
CO5	Analyze wireless network security using authentication-bypass, attack-simulation, and traffic-analysis techniques.	L4

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	H		H	M	H	M
CO2	M		H	M	H	M
CO3	H		H	H	H	H
CO4	M		H	H	H	H
CO5	H		H	H	H	H

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	Contact Hours
UNIT – 1	Introduction-Penetration Testing phases/Testing Process, types and Techniques, Blue/Red Teaming, Strategies of Testing, Non-Disclosure Agreement checklist, Phases of hacking, Open-source/proprietary Pentest methodologies.	12
UNIT – 2	Information Gathering and Scanning-Information gathering methodologies- Foot printing, Competitive Intelligence- DNS Enumerations- Social Engineering attacks, Port Scanning- Network Scanning-Vulnerability Scanning-NMAP scanning tool-OS Fingerprinting- Enumeration.	12
UNIT – 3	System Hacking Password cracking techniques- Key loggers- Escalating privileges- Hiding Files, Double Encoding, Steganography technologies and its countermeasures. Active and passive sniffing- ARP Poisoning, MAC Flooding- SQL Injection - Error- based, Union-based, Time -based, Blind SQL, Out-of-band. Injection Prevention Techniques.	12
UNIT – 4	Advanced System Hacking: Broken Authentication, Sensitive Data Exposure, XML External Entities, Broken Access Code, XSS - Stored, Reflected, DOM Based.	12
UNIT – 5	**Wireless Pentest:** Wi-Fi Authentication Modes, Bypassing WLAN Authentication, Types of Wireless Encryption, WLAN Encryption Flaws, AP Attack, Attacks on the WLAN Infrastructure, DoS-Layer1, Layer2, Layer 3, DDoS Attack, Client Mis-association, Wireless-Hacking Methodology, Wireless Traffic Analysis.	12
	Total	60

Text Books:

1. Kali Linux
2. Windows Penetration Testing, 1st Edition, By Wolf Halton, Bo Weaver, June 2016 ,Packt Publishing

Reference Books:

1. Mastering Modern Web Penetration Testing By Prakhar Prasad, October 2016 Packt Publishing.
2. SQL Injection Attacks and Defense 1st Edition, by Justin Clarke-Salt, Syngress Publication.

II Semester	D2522602- MALWARE ANALYSIS & REVERSE ENGINEERING	L	T	P	C
		3	1	0	4

Course Objectives:

- To understand the purpose of computer infection program.
- To implement the covert channel and mechanisms.
- To test and exploit various malware in open source environment.
- To analyze and design the famous virus and worms.
- Understand the Reverse Engineering (RE) Methodology
- Disassemble products and specify the interactions between its subsystems and their functionality.

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (L)#
CO1	Explain the characteristics of Malware and its effects on Computing systems.	L2
CO2	Identify system vulnerabilities and perform basic Malware analysis using appropriate tools.	L3
CO3	Analyze the given Portable Executable and Non-Portable Executable files using Static and dynamic analysis techniques.	L4
CO4	Demonstrate the Malware functionalities.	L3
CO5	Analyze malware using reverse engineering, identify its indicators, and classify it using signatures.	L3

- #Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		H	M	H	M
CO2	H		H	H	H	H
CO3	H		H	H	H	H
CO4	M		H	H	H	H
CO5	H		H	H	H	H

- (Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	**Contact Hours**
UNIT – 1	**Malware Basics**- General Aspect of Computer infection program, Non Self Reproducing Malware, How does Virus Operate, Virus Nomenclature, Worm Nomenclature, Recent Malware Case Studies.	12
UNIT – 2	**Basic Analysis-** Antivirus Scanning, x86 Disassembly, Hashing, Finding Strings, Packed Malware, PE File Format, Linked Libraries & Functions, PE Header File &Section.	12
UNIT – 3	**Advanced Static & Dynamic Analysis**-IDA Pro, Recognizing C code constructs, Analyzing malicious windows program, Debugging, OllyDbg, Kernel Debugging with WinDbg, Malware Focused Network Signatures.	12
UNIT – 4	**Malware Functionalities-**Malware Behavior, Covert Malware Launch, Data Encoding, Shell code Analysis.	12
UNIT – 5	**Reverse Engineering Malware (REM)**: REM Methodology, Resources for Reverse-Engineering Malware (REM) Understanding Malware Threats, Malware indicators, Malware Classification, Examining Clam AV-Signatures.	12
	Total	60

Text books:

1. Michael Sikorski, Andrew Honig "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" publisher Williampollock

Reference Books:

1. ErciFiliol, "Computer Viruses: from theory to applications", Springer, 1st edition, 2005.

II Semester	D2522603- CYBER CRIME INVESTIGATION & DIGITAL FORENSICS	L	T	P	C
		3	1	0	4

Course Objectives:

- To identify security risks and take preventive steps
- To understand the forensics fundamentals.
- To understand the evidence capturing process.
- To understand the preservation of digital evidence

Course Outcomes: On completion of this course, the student will be able to:

	CO Statement	Knowledge Level (K)#
CO1	Acquire the definition of computer forensics fundamentals.	L2
CO2	Describe the types of computer forensics technology	L2
CO3	Analyze various computer forensics systems.	L4
CO4	Illustrate the methods for data recovery, evidence collection and data seizure.	L2
CO5	Summarize duplication and preservation of digital evidence.	L2

- #Based on suggested Revised BTL
- Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		H	M		M
CO2	M		H	M		M
CO3	H		H	H		H
CO4	H		H	H		H
CO5	M		H	M		H

- (Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	Contact Hours
UNIT – 1	**Introduction:** Overview of Cyber Crime, Nature and Scope, Types (Social Engineering), Categories of Cyber Crime, Property Cyber Crime.	12
UNIT – 2	**Cyber Crime Issues**: Unauthorized Access, Computer Intrusions, White-collar Crimes, Viruses/Malicious Code, Hacking/Cracking, Software Piracy, Intellectual Property, Stalking/Obscenity, Law Enforcement Roles and Responses.	12

UNIT – 3	**Investigation:** Introduction, Tools, e-Discovery, Digital Evidence Collection/Preservation, E-Mail/IP Tracking, Recovery, Case Studies, Encryption/Decryption Methods, Search and Seizure of Computers, Recovery of Deleted Evidence, and Password Cracking.	12
UNIT – 4	**Digital Forensics:** Forensic Software and Hardware, Analysis and Advanced Tools, Forensic Technology and Practices, Forensic Ballistics and Photography, Biometrics (Face, Iris, Fingerprint), Audio/Video Analysis, OS Forensics (Windows/Linux), Network Forensics.	12
UNIT – 5	**Laws and Acts:** Laws and Ethics, Digital Evidence Controls, Indian Evidence Handling Procedure, Indian Evidence ACT, IPC and CrPC, Electronic Communication Privacy ACT, Legal Policies.	12
	Total	60

Reference Books:

1. Nelson Phillips and Enfinger Steuart, "Computer Forensics and Investigations", Cengage Learning, New Delhi, 2009.
2. Kevin Mandia, Chris Prosise, Matt Pepe, "Incident Response and Computer Forensics", Tata McGraw-Hill, New Delhi, 2006.

Robert M Slade," Software Forensics", Tata McGraw - Hill, New Delhi, 2005.

II Semester	D25226A0- CLOUD AND IoT SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

- Student learn and understand the advantages, challenges, security issues of cloud computing and interrelationships between cloud computing and big data.
- Students learn different Key components of Amazon Web Services, Cloud Backup and solutions.
- Student able to discuss the main threats and attacks on IoT products and services
- Be able to learn secure a connected IoT product from scratch.

Course Outcomes: On completion of this course, the student will be able to:

CO	Course Outcome	Knowledge Level (L)
CO1	Understand the fundamentals of Cloud Computing including cloud deployment models, service models, benefits, challenges, and virtualization concepts.	L2
CO2	Apply cloud application development concepts using platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform with appropriate security and availability management techniques.	L3
CO3	Understand the architecture, technologies, communication models, and application layer protocols involved in the Internet of Things ecosystem.	L2
CO4	Analyze IoT system design principles, business models, communication technologies, and IoT/M2M layered architectures for connected device applications.	L4
CO5	Analyze IoT security requirements and suitable mechanisms for device authentication, secure communication, privacy protection, vulnerability management, and high availability.	L4

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		H	M		M
CO2	M		H	M		M
CO3	H		H	H		H
CO4	H		H	H		H
CO5	M		H	M		H

- (Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	**Contact Hours**
UNIT – 1	**Cloud Computing Fundamental-**Cloud Computing definition, private, public and hybrid cloud. Cloud types; IaaS, PaaS, SaaS. Benefits and challenges of cloud computing, public vs private clouds, role of virtualization in enabling the cloud	12
UNIT – 2	**Cloud Applications-**Development environments for service development; Amazon, Azure, Google App. Security management in the cloud – security management standards- SaaS, PaaS, IaaS availability management- access control- Data security and storage in cloud	12
UNIT – 3	**The Internet of Things-**An Overview of Internet of things, Internet of Things Technology, behind IoTs Sources of the IoTs, M2M Communication, Examples of IoTs, Design Principles for Connected Devices, Internet Connectivity Principles, Internet connectivity, Application Layer Protocols: HTTP, HTTPS, FTP, Telnet	12
UNIT – 4	**IOT Design**-Business Models for Business Processes in the Internet of Things, IoT/M2M systems layers and designs standardizations, Modified OSI Stack for the IoT/M2M Systems, ETSI M2M domains and High-level capabilities, Communication Technologies, Data Enrichment and Consolidation and Device Management Gateway Ease of designing and affordability	12
UNIT – 5	**IOT Security Issues-** Secure constrained devices, Authorize and authenticate devices, Manage device updates, secure communication, Ensure data privacy and integrity, secure web, mobile, and cloud applications, Ensure high availability**,** Detect vulnerabilities and incidents, Manage vulnerabilities, Predict and preempt security issues.	12
	Total	60

Text Books:

1. Internet of Things: Architecture, Design Principles and Applications, Raj kamal, McGraw Hill Higher Education
2. Internet of Things, A. Bahgya and V. Madisetti, Univesity Press, 2015

Reference Books:

1. Gautam Shroff, Enterprise Cloud Computing Technology Architecture Applications
2. Toby Velte, Anthony Velte, Robert Elsenpeter, Cloud Computing, A Practical Approach
3. IOT Security Issues by Alasdair Gilchrist, O'Reilly Publishers, 2017.
4. Tim Mather, Subra Kumara swamy, Shahed Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance.

II Semester	D25226A1- AI FOR CYBER SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

The course is taught with the objectives of enabling the student to:

- Understand the importance of AI in cyber security and their limitations
- Understand detection methods for image spam and threat analysis
- Apply Time Series Analysis and Ensemble Modeling in practical applications
- Perform experiments Using Data Science to Catch Email Fraud and Spam

Course Outcomes: On completion of this course, the student will be able to:

CO	Course Outcome	Knowledge Level (L)
CO1	Understand the fundamentals of Artificial Intelligence and its applications in cybersecurity, including evolution, learning types, and algorithm training concepts.	L2
CO2	Apply AI techniques such as classification, NLP, and machine learning models to detect cyber threats including spam, phishing, and image-based attacks.	L3
CO3	Apply machine learning, time series analysis, and ensemble methods to analyze and predict cybersecurity attacks such as DDoS.	L3
CO4	Apply heuristic and machine learning techniques to identify malicious URLs and analyze CAPTCHA mechanisms using AI methods.	L3
CO5	Apply machine learning and data science techniques for fraud detection in emails and networks using modern tools and cloud-based AI solutions.	L3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	H		H	H	H	M
CO2	H		H	H	H	H
CO3	H		H	H		
CO4	M		H	H	H	H
CO5	H		H	H	H	H

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	Contact Hours
UNIT – 1	Introduction to AI for Cyber security Applying AI in cyber security, The evolution from expert systems to data mining and AI, The different forms of automated learning, The characteristics of algorithm training and optimization, Introducing AI in the context of cyber security.	12
UNIT – 2	AI for Cyber security Arsenal Classification, Regression, Dimensionality reduction, Clustering, Speech recognition, Video	12

	anomaly detection, Natural language processing (NLP), Large-scale image processing, Social media analysisDetecting Cyber security Threats with AI, How to detect spam with Perceptrons, Image spam detection with Support Vector Machines (SVMs), Phishing detection with logistic regression and decision trees, Spam detection with Naive Bayes, Spam detection adoptingNLP.	
UNIT – 3	Basics of Machine Learning in Cyber security, Delving into machine learning in the cyber security world, Different types of machine learning systems, Different data preparation techniques, Machine learning architecture, statistical models and machine learning models, Model tuning to ensure model performance and accuracy, Machine learning toolsTime Series Analysis and Ensemble Modeling Time series and its different classes, Time series decomposition, Analysis of time series in cyber security, Prediction of DDoS attack, Ensemble learning methods and voting ensemble methods to detect cyber-attacks.	12
UNIT – 4	Segregating Legitimate and Lousy URLs Understanding URLs and how they fit in the internet address scheme, Introducing malicious URLs, Looking at the different ways malicious URLs propagate, Using heuristics to detect malicious URLs, Using machine learning to detect malicious URLsKnocking Down CAPTCHAs Characteristics of CAPTCHAs, Using artificial intelligence to crack CAPTCHAs, Types of CAPTCHA, Solving CAPTCHAs with neural networks.	12
UNIT – 5	Fraud Prevention with Cloud AI Solutions How to leverage machine learning (ML) algorithms for fraud detection, How bagging and boosting techniques can improve an algorithm's effectiveness, How to analyze data with IBM Watson and JupyterNotebook,Using Data Science to Catch Email Fraud and Spam and Efficient Network Anomaly Detection Using k-means Fraudulent emails and spoofs, Types of email fraud, Spam detection using the Naive Bayes algorithm, Featurization techniques that convert text-based emails into numeric values, Spam detection with logistic regression.	12
	Total	60

Text Books:

1. Alessandro Parisi, Hands-On Artificial Intelligence for Cyber security: Implement smart AI systems for preventing cyber-attacks and detecting threats and network anomalies, Packt Publication, 2019.

Reference Books:

1. Clarence Chio and David Freeman, Machine Learning and Security: Protecting Systems with Data and Algorithms O‟REILLY Publications, 2018.
2. McKinney, W Brij B. Gupta and Quan Z. Sheng, Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices (Cyber Ecosystem and Security), CRC Press Publication, 2019.

II Semester	D25226A2- DATA PRIVACY	L	T	P	C
		3	0	0	3

Course Objectives:

- The objective of this course is to create architectural, algorithmic and technological foundations for the maintenance of the privacy of individuals
- Student able to learn the concepts of confidentiality of organizations, and the protection of sensitive information, despite the requirement that information be released publicly or semi-publicly.

Course Outcomes: On completion of this course, the student will be able to:

	Course Outcome	Knowledge Level (K)#
CO1	Understand basic privacy concepts, data privacy attacks, access control models, and privacy policies in various domains.	L2
CO2	Analyze data explosion challenges and apply mathematical and protection models to safeguard personal information	L4
CO3	Evaluate privacy protection techniques, disclosure control methods, and their strengths and weaknesses.	L4
CO4	Apply computational tools and methods to protect structured and textual data.	L3
CO5	Analyze web privacy issues and related legal protections under the Freedom of Information Act and search warrant requirements.	L4

- #Based on suggested Revised BTL
- Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		H	M	H	M
CO2	H		H	H	H	M
CO3	H		H	H	H	M
CO4	M		H	H	H	M
CO5	H		H	M	H	H

- (Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	Contact Hours
UNIT – 1	**Introduction**- Fundamental Concepts, Definitions, Statistics, Data Privacy Attacks, Data linking and profiling, access control models, role-based access control, privacy policies, their specifications, languages and implementation, privacy	12

	policy languages, privacy in different domains- medical, financial, etc.	
UNIT – 2	**Data explosion**- Statistics and Lack of barriers in Collection and Distribution of Person-specific information, Mathematical model for characterizing and comparing real-world data sharing practices and policies and for computing privacy and risk measurements, Demographics and Uniqueness, **Protection Models**- Null-map, k-map, Wrong map	12
UNIT – 3	**Survey of techniques**- Protection models (null-map, k-map, wrong map), Disclosure control, Inferring entity identities, Strength and weaknesses of techniques, entry specific databases.	12
UNIT – 4	**Computation systems for protecting delimited data**- MinGen, Datafly, Mu-Argus, k-Similar, Protecting textual documents: Scrub.	12
UNIT – 5	**Technology, Policy, Privacy and Freedom**- Medical privacy legislation, policies and best practices, Examination of privacy matters specific to the World Wide Web, Protections provided by the Freedom of Information Act or the requirement for search warrants.	12
	Total	60

Text Books:

1. B. Raghunathan, The Complete Book of Data Anonymization: From Planning to Implementation,1st Edition, Auerbach Pub, 2013.
2. L. Sweeney, Computational Disclosure Control: A Primer on Data Privacy Protection, MIT Computer Science, 2002.

II Semester	D25226B0- PRINCIPLES OF SECURE CODING	L	T	P	C
		3	0	0	3

Course Objectives:

- Understanding of the various security attacks and knowledge to recognize and remove common coding errors that lead to vulnerabilities.
- Knowledge of outline of the techniques for developing a secure application.
- Recognize opportunities to apply secure coding principles.

Course Outcomes: On completion of this course, the student will be able to:

CO	Course Outcome	Knowledge Level (L)
CO1	Explain secure systems and various security attacks.	L2
CO2	Demonstrate the software development process incorporating secure coding practices.	L3
CO3	Apply secure programming techniques to identify and mitigate various software risks.	L3
CO4	Analyze various errors that lead to software vulnerabilities.	L4
CO5	Analyze real-time software vulnerabilities and security requirements.	L4

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		H	M	H	M
CO2	H		H	H	H	M
CO3	H		H	H	H	H
CO4	M		H	H	H	M
CO5	H		H	H	H	H

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	Contact Hours
UNIT – 1	**Introduction:** Need for secure systems, Proactive security development process, Security principles to live by and threat modelling.	12
UNIT – 2	**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	12

UNIT – 3	**Secure Coding in C++ and Java:** Dynamic memory management, Common errors in dynamic memory management, Memory managers, Double –free vulnerabilities, Integer security, Mitigation strategies	12
UNIT – 4	**Database and Web Specific Input Issues:** Quoting the Input, Use of stored procedures, Building SQL statements securely, XSS related attacks and remedies	12
UNIT – 5	**Software Security Engineering:** Requirements engineering for secure software: Misuse and abuse cases, SQUARE process model Software security practices and knowledge for architecture and design	12
	Total	60

Text Book:

1. Michael Howard, David LeBlanc, "Writing Secure Code", Microsoft Press, 2nd Edition, 2003.

Reference Books:

1. Robert C. Seacord, "Secure Coding in C and C++", Pearson Education, 2nd edition, 2013.
2. 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, 2008.

II Semester	D25226B1- SECURITY ASSESSMENT AND RISK ANALYSIS	L	T	P	C
		3	0	0	3

Course Objectives

- Student able to learn basic concepts of risk management
- Integrate the IRP, DRP, and BCP plans into a coherent strategy to support sustained organizational operations.
- Able understand and discuss incident response options, and design an Incident Response Plan for sustained organizational operations.

Course Outcomes: On completion of this course, the student will be able to:

CO No.	Course Outcome	Bloom's Level
CO1	Explain the fundamentals of information security, security services, threats, vulnerabilities, and security countermeasures.	**L2 – Understand**
CO2	Analyze different types of system threats, vulnerabilities, and risk management techniques for securing information systems.	**L4 – Analyze**
CO3	Apply security planning, risk assessment, contingency planning, and disaster recovery mechanisms in organizational environments.	**L3 – Apply**
CO4	Demonstrate knowledge of physical, personnel, and administrative security controls along with auditing and monitoring techniques.	**L3 – Apply**
CO5	Understand operations security concepts, cryptographic techniques, key management, and computer security mechanisms.	**L2 – Understand**

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		H	M	H	H
CO2	H		H	M	H	H
CO3	H		H	H	H	H
CO4	M		H	H	H	M
CO5	H		H	H	H	H

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	**Contact Hours**
UNIT – 1	**Security Basics**-Information Security (INFOSEC) Overview: critical information characteristics – availability information states – processing security counter measures education, training and awareness, critical information 1characteristics – confidentiality critical information characteristics – integrity, information states – storage, information states – transmission, security counter measures policy, procedures and practices, threats, vulnerabilities.	12
UNIT – 2	**Threats to and Vulnerabilities of Systems**: definition of terms (e.g., threats, vulnerabilities, risk), major categories of threats (e.g., fraud, Hostile Intelligence Service (HOIS), malicious logic, hackers, environmental and technological hazards, disgruntled employees, careless employees, HUMINT, and monitoring), threat impact areas, Countermeasures: assessments (e.g., surveys, inspections), Concepts of Risk Management: consequences (e.g., corrective action, risk assessment), cost/benefit analysis of controls, implementation of cost effective controls, monitoring the efficiency and effectiveness of controls (e.g., unauthorized or inadvertent disclosure of information), threat and vulnerability assessment	12
UNIT – 3	**Security Planning: directives and procedures for policy mechanism, Risk Management:** acceptance of risk (accreditation), corrective actions information identification, risk analysis and/or vulnerability assessment components, risk analysis results evaluation, roles and responsibilities of all the players in the risk analysis process, Contingency Planning/Disaster Recovery: agency response procedures and continuity of operations, contingency plan components, determination of backup requirements, development of plans for recovery actions after a disruptive event, development of procedures for offsite processing, emergency destruction procedures, guidelines for determining critical and essential workload, team member responsibilities in responding to an emergency situation	12
UNIT – 4	**Policies And Procedures**: Physical Security Measures: alarms, building construction, cabling, communications centre, environmental controls (humidity and air conditioning), filtered power, physical access control systems (key cards, locks and alarms) Personnel Security Practices and Procedures: access authorization/verification (need to know), contractors, employee clearances, position sensitivity, security training and awareness, systems maintenance personnel, Administrative Security Procedural Controls: attribution, copyright protection and licensing , Auditing and Monitoring: conducting security reviews, effectiveness of security programs, investigation of security breaches, privacy review of accountability controls, review of audit trails and Logs	12

UNIT – 5	Operations Security (OPSEC): OPSEC surveys/OPSEC planning INFOSEC: computer security – audit, cryptography encryption (e.g., point to point, network, link), cryptography key management (to Include electronic key), cryptography strength (e.g., complexity, secrecy, characteristics of the key) Case study of threat and vulnerability assessment	12
	Total 60	

Text Books:

1. Principles of Incident Response and Disaster Recovery, 1st Edition, Whitman & Mattord, Course Technology,2006

Web Link Reference:http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf

II Semester	D25226B2- BIOMETRIC SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

- Introduce Bio-metric and traditional authentication methods.
- Describe the background theory and types of features used in biometric techniques and algorithms related to various biometrics.
- Evaluate the performance of various biometric systems.

Course Outcomes: On completion of this course, the student will be able to:

CO	Course Outcome	Knowledge Level (L)
CO1	Describe the various modules constituting a biometric system. Compare and contrast different biometric traits and appreciate their relative significance.	L2 (Understand)
CO2	Classify the different feature sets used to represent some of the popular biometric traits.	L4 (Analyze)
CO3	Analyze security systems incorporating biometric technologies and identify suitable security requirements.	L4 (Analyze)
CO4	Apply multi-biometric and multi-factor methods to authenticate users and protect biometric data.	L3 (Apply)
CO5	Analyze biometric technologies, applications, vulnerabilities, and legal aspects in various sectors.	L4 (Analyze)

#Based on suggested Revised BTL

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		H	M	H	M
CO2	M		H	H	H	M
CO3	H		H	H	H	H
CO4	H		H	H	H	H
CO5	H		H	M	H	H

UNIT	CONTENTS	Contact Hours
UNIT – 1	Introduction and Definitions of Biometrics; Traditional Authentication Methods and Technologies. Introduction to Image Processing and Image Enhancement Techniques. Spatial Domain Methods: Smoothing Filters, Sharpening Filters and Laplacian Filters. Frequency Domain Methods: Smoothing and Sharpening Filters.	12
UNIT – 2	Image Restoration and Reconstruction: Models of Image Degradation and Restoration Processes, Noise Models, Spatial Filtering Techniques, Inverse Filtering, and Minimum Mean Square Error (MMSE) Filtering. Introduction to Image Segmentation. Edge Detection in Images: Concepts and Types of Edge Detectors. Introduction to Image Feature Extraction.	12
UNIT – 3	Biometric Technologies: Fingerprint, Face, Iris, Hand Geometry, Gait, Ear, Voice, Palm Print and Online Signature Recognition Techniques; 3D Face Recognition, Dental Identification, and DNA Biometrics.	12

UNIT – 4	Legal Aspects and Use of Multibiometric Systems. Statistical Evaluation and Performance Measures of Biometric Systems. Applications of Biometrics in Government and Commercial Sectors. Case Studies of Biometric Systems and Biometric Transactions. Vulnerabilities in Biometric Systems. Recent Trends in Biometric Technologies and Their Applications across Various Domains. Case Studies on 3D Face Recognition and DNA Matching.	12
UNIT – 5	Signature and Handwriting Technologies: Technical Description, Classification, Keyboard/Keystroke Dynamics, Voice Biometrics, Data Acquisition Techniques, Feature Extraction, Characteristics, Strengths, Weaknesses, and Deployment Issues. Multibiometric and Multifactor Authentication Systems: Two-Factor Authentication using Passwords, Tickets, and Tokens; Executive Decision-Making and Implementation Planning.	12
	Total	60

Suggested Readings:

1. Reid, P. (2004). Biometrics for network security, Pearson Education.
2. Maltoni, D., Maio, D., Jain, A.K., and Prabhakar, S. (2003). Handbook of Fingerprint Recognition. Springer-Verlag.
3. Jain, A. K., Bolle, R., and Pankanti S. (1999). BIOMETRICS: Personal Identification in Networked Society. Kluwer Academic Publishers.
4. Jain, A. K., Ross, A. A., &kumar, K. N. (2011). Introduction to Biometrics, Springer.
5. Jain, A. K., Maltoni, D., and Maio, D. (2005). Biometric Systems: Technology, Design and Performance Evaluation. Springer.
6. Gonzalez, R. C., and Woods, R. E. (2018). Digital Image Processing India: Pearson Education.
7. Research Articles from SCI & Scopus indexed Journals.

II Semester	D2522690- VULNERABILITY ASSESSMENT & PENETRATION TESTING LAB	L	T	P	C
		0	1	2	2

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Apply penetration testing methodologies and security tools to identify and analyze system, network, and web application vulnerabilities.	L3
CO2	Apply common web and network attack techniques such as SQL Injection, XSS, CSRF, port scanning, and packet analysis to assess security weaknesses.	L3
CO3	Evaluate advanced exploitation and post-exploitation techniques using frameworks, rootkits, tunneling, and traffic analysis methods	L5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	H		H	H	H	H
CO2	M		H	H	H	H
CO3	H		H	H	H	H

(Please fill the above with Levels of Correlation, viz., L, M, H)

Experiment	CONTENTS
Experiment 1:	Implement penetration testing and phases of penetration testing.
Experiment 2:	Make use of different types of tools available in kali and parrot O.S.
Experiment 3:	Practice different SQL injection attacks.
Experiment 4:	Implement and use GHDBC and Microsoft Vulnerabilities (Common CVE).
Experiment 5:	Implement Exploit insecure file handling, upload web shells, deface using upload file mechanism.
Experiment 6:	Perform XSS attacks on client-side application
Experiment 7:	Implement a case on actions on behalf users by CSRF, Test websites for Clickjacking.

Experiment 8:	Implement port scanning by using NMAP and other tools to find the open ports.
Experiment 9:	Text for wire shark and Tcpdumps to analyze various types of packets
Experiment 10:	Implement Password attacks with methods like Dictionary Files - Key-space Brute Force - Pwdump and Fgdump - Windows Credential Editor (WCE- Exercises - Password Profiling - Password Mutating
Experiment 11:	Implement Metasploit frameworks.
Experiment 12:	Implement Trojan horse root kits backdoors.
Experiment 13:	Practice ARP spoofing and buffer overflow exploitation with ETERCAP and SHELL'S.
Experiment 14:	Perform Port Redirection, SSL Encapsulation - Stunnel, HTTP CONNECT Tunneling, Proxy Tunnel, SSH Tunneling.

List of open-Source software/learning Websites:

1. https://www.hackthebox.eu/
2. https://practicalpentestlabs.com/
3. https://pentesterlab.com

II Semester	D2522691- DIGITAL FORENSICS LAB	L	T	P	C
		0	1	2	2

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Apply forensic tools and techniques to recover deleted files and create forensic disk images.	L3
CO2	Collect, preserve, and analyze digital evidence from emails, browsers, and USB devices	L3
CO3	Perform live forensic investigations using specialized tools to capture and analyze system activity	L3
CO4	Analyze network traffic and packet data using Wireshark to extract forensic evidence.	L4
CO5	Use system monitoring tools to track processes, network activity, and memory usage for forensic purposes.	L3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	H		H	H		H
CO2	H		H	H		H
CO3	H		H	H		H
CO4	M		H	H		H
CO5	M		H	H		H

(Please fill the above with Levels of Correlation, viz., L, M, H)

Experiment	CONTENTS
Experiment-1	Study of Computer Forensics and different tools used for forensic investigation
Experiment-2	How to Recover Deleted Files using Forensics Tools
Experiment-3	How to make the forensic image of the hard drive using EnCase Forensics.
Experiment-4	How to Collect Email Evidence in Victim PC
Experiment-5	How to Extracting Browser Artifacts
Experiment-6	Find Last Connected USB on your system (USB Forensics)
Experiment-7	Live Forensics Case Investigation using Autopsy
Experiment-8	Capturing and analyzing network packets using Wireshark
Experiment-9	Analyze the packets provided in lab and solve the questions using Wireshark a) What web server software is used by www.uceou.com

	b) About what cell phone problem is the client concerned? c) How many webservers are running in Apache webserver.
Experiment-10	Using Sysinternals tools for Network Tracking and Process Monitoring • Check Sysinternals tools • Monitor Live Processes • Capture RAM • Capture TCP/UDP packets • Monitor Hard Disk • Monitor Virtual Memory • Monitor Cache Memory
Experiment-11	Email Forensics • Mail Service Providers • Email protocols • Recovering emails • Analyzing email header
Experiment-12	Analyzing data of android mobile using MOBILedit.