Francis Xavier Engineering College

(An Autonomous Institution)
Tirunelveli - 627 003
Tamil Nadu India

Department of Computer Science and Engineering

Curriculum and Syllabi – 2021-UG

CHOICE BASED CREDIT SYSTEM AND OBE

B.E. – Computer Science and Engineering

(Specialization in Cyber Security)

Vision of the Department

To become a center of excellence in Computer Science and Engineering and Research to create global leaders with holistic growth and ethical values for the industry and academics.

Mission of the Department

- To produce technocrats in the industry and academia by educating computer concepts and techniques.
- To facilitate the students to trigger more creativity by applying modern tools and technologies in the field of Computer science and Engineering
- To inculcate the spirit of ethical values contributing to the welfare of the society

Summary

S. No	Course Code	Course Name	L	T	P	C	H
Theory Course							
1	21CS4S01	Cyber Security Management And Cyber Law	3	0	0	3	3
		Elective	3	0	0	3	3
Theory cum Practical Courses							
1	21CS5S01	Cyber Security Essentials	2	0	4	4	4
3	21CS6S01	Forensics and Incident Response	2	0	4	4	4
Practical Course							
1.	21CS8S11	Project work	0	0	8	4	8
		Total	10	0	16	**18**	22
Elective Courses							
1	21CS7S01	Cloud Security	3	0	0	3	3
2	21CS7S02	Database Security	3	0	0	3	3
3	21CS7S03	Mobile And Wireless Security	3	0	0	3	3

21CS4S01 CYBER SECURITY MANAGEMENT AND CYBER LAW L T P C 3 0 0 3

Course Objectives:

- To understand the nature of threats and cyber security management goals technology
- To understand the landscape of hacking and perimeter defense mechanisms
- To develop strategies for cyber security and protecting critical infrastructure
- To understand policies to mitigate cyber risks and digital signature
- To understand the IT Act, scheme, amendments, IPR and emerging cyber law and desired cyber ecosystem capabilities

PRE-REQUISITE:

- **Nil**

UNIT I **10**

Introduction- Cyberspace , Cyber Crime, Nature of Threat, Cyber security, Cyber security Policy, Mission and Vision of Cyber security Program. Cyber security management system- goals, technology categories – perimeter defense and encryption. Cyber security management framework.

UNIT II **8**

Introduction to Hacker Means, Social Engineering, Scanners, password Cracking, IP Spoofing Trojan Horses. Case study: an example of how a bank/plant was hacked. The Cyber Security Management System: Policy - Password Management, Anti-Virus, Incident Handling, Backup and Recovery, Proprietary Information. Technology - Perimeter Defense, Types of Network Security Devices -Firewalls, Intrusion Detection Systems, Content Filtering, Virtual Private Networks, Encryption.

UNIT III **9**

STRATEGIES FOR CYBER SECURITY -Creating a Secure Cyber, Types of Attacks , Comparison of Attacks , Creating an Assurance Framework, Encouraging Open Standards, Strengthening the Regulatory framework, Creating Mechanisms for IT Security, Securing E-Governance Services, Protecting Critical Information Infrastructure.

UNIT IV **9**

POLICIES TO MITIGATE CYBER RISK -Promotion of R&D in Cyber security, Reducing Supply Chain Risks, Mitigate Risks through Human Resource Development, Creating Cyber security Awareness, Information sharing Implementing a Cyber security Framework. SIGNATURES - Digital Signature ,Electronic Signature, Digital Signature to Electronic.

UNIT V **9**

Information Technology Act: Salient Features, Scheme, Application of the I.T. Act ,Amendments I.T. Act , Offences, Compounding of Offences. INTELLECTUAL PROPERTY RIGHTS: Types of Intellectual Property Rights, Intellectual Property Rights in India, Intellectual Property in Cyber Space. Emerging Trends of Cyber Law. Desired Cyber Ecosystem Capabilities.

Total: 45 Periods

REFERENCE BOOK(S):

1. Cyber Security Best Practices Guide For IIROC Dealers Members, Canada.
2. NIST Cyber security Framework, Version 1.0, 2014
3. CGI, ―Cyber security in Modern Critical Infrastructure Environments,‖ 2014
4. John H. Dexter , ―The Cyber Security Management System – A Conceptual Mapping‖, The SANs Institute, 2002
5. Peter Trim and Yang-Im Lee, ―Cyber Security Management- A Governance, Risk and Compliance Framework‖, Gower Publishing, England 2014
6. Stuart Broderick J , Cyber Security Program, Cisco Security Solutions, June 2016
7. www.Tutorialspoint.com,Information Security and Cyber Law,Tutorials Point (I) Pvt. Ltd, 2015

WEB RESOURCE(S):

1. https://www.slideshare.net/Utchi/cyberspace-59476434
2. https://slideplayer.com/slide/12853278/
3. https://www.slideshare.net/ShravanSanidhya1/presentation-on-ethical-hacking-ppt

COURSE OUTCOME(S):

1. Gain knowledge on the nature of threats and cyber security management goals and framework
2. Knowledge on the landscape of hacking and perimeter defense mechanisms
3. Ability to differentiate and integrate strategies for cyber security and protecting critical infrastructure
4. Able to understand policies to mitigate cyber risks
5. Knowledge on IT Act, and amendments, copy rights, IPR and cyber law to deal with offenses.

PO Vs CO MAPPING:

CO No	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	3	3		3								2
2	2	3		3								
3	2			3								
4	2	3		3								
5	1	1		1				2		2		

1→Low 2→Medium 3→High

21CS5S01 CYBER SECURITY ESSENTIALS L T P C

2 0 4 4

Course Objectives:

Understand the field of digital security and concepts of access control mechanism.

- To introduce the need for cyber security
- To introduce keywords and jargons involved in securing browser
- Understanding network basic and familiarize on security of network protocols
- Awareness and understanding on cyber-attacks and data privacy
- Understand the principles of data security

PRE-REQUISITE:

- Nil.

UNIT I **6**

The Need for Cyber Security-Personal Data- Organization Data- Attackers and Cyber Security Professionals-Cyber warfare

UNIT II **6**

Basics of digital security, protecting personal computers and devices, protecting devices from Virus and Malware, Identity, Authentication and Authorization, need for strong credentials, Keeping credentials secure, Protecting servers using physical and logical security, World Wide Web (www), the Internet and the HTTP protocol, security of browser to web server interaction

UNIT III **6**

Networking basics (home network and large-scale business networks), Networking protocols, Security of protocols, sample application hosted on-premises.

UNIT IV **6**

Introduction to cyber-attacks, application security (design, development and testing), operations security, monitoring, identifying threats and remediating them.

UNIT V **6**

Principles of data security - Confidentiality, Integrity and Availability, Data Privacy, Data breaches, preventing attacks and breaches with security controls, Compliance standards, Computer Ethics.

Total Theory Hours: 30 Periods

LABORATORY EXPERIMENTS:

1. Setup a honey pot and monitor the honey pot on network.
2. Write a script or code to demonstrate SQL injection attacks.
3. Create a social networking website login page using phishing techniques.
4. Write a code to demonstrate DoS attacks.
5. Install rootkits and study variety of options.

Total Lab hours: 15 Periods
Total Hours: 45 Periods

Text Books:

1. Sammons, John, and Michael Cross. The basics of cyber safety: computer and mobile device safety made easy. Elsevier, 2016.

References:

1. Charles P. Pfleeger, Shari Lawrence, Pfleeger Jonathan Margulies; Security in Computing, Pearson Education Inc . 5th Edition,2015
2. Brooks, Charles J., Christopher Grow, Philip Craig, and Donald Short. Cyber security essentials. John Wiley & Sons,2018
3. CISCO Networking Academy,"Introduction to Cyber Security"

WEB RESOURCE(S):

1. https://geekflare.com/understanding-cybersecurity
2. https://www.geeksforgeeks.org/basics-computer-networking
3. https://www.ramsac.com/services/cybersecurity/an-introduction-to-cyber-attacks
4. https://www.slideshare.net/Siblu28/cyber-security-36922359

Course Outcomes

Upon completion of the course, the students will be able to

CO1: Apply a solid foundation in digital security and measures taken to protect device from threats.

CO2: Learning access control mechanism and understand how to protect servers

CO3: Understand the importance of a network basics and brief introduction on security of network Protocols

CO4: To understand cyber-attacks and learn data privacy issues and preventive measures

CO5: Listen and comprehend lectures and talks in their area of specialization successfully.

PO vs CO Mapping

CO No	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	3	2		1								
2	2	2		2								2
3	3	1										
4	3	3		1								
5	3									2		2

1→Low 2→Medium 3→High

21CS6S01 FORENSICS AND INCIDENT RESPONSE L T P C

2 0 4 4

Course Objectives:

- Gain knowledge on the basics of procedures for identification, preservation of electronic evidence.
- Understand the purpose and usage of various forensic tools.
- Gain knowledge on how scientific evidence collection/extraction during investigation.
- Acquire knowledge on file systems and its inner working.
- Understand the windows and linux investigation procedures.
- Introduce the report writing guidelines and principles.

Pre-requisite Courses:

- Nil

UNIT I **6**

Introduction to Incident - Goals of Incident Response- Introduction to Incident Response Methodology (IRM)- Steps in Incident Response Methodology- IRM: Pre-incident preparation-IRM: Detection of incidents- IRM: Initial Response- IRM: Formulate a Response Strategy- IRM: Investigate the Incident-IRM: Reporting- Creating response toolkit – Windows-Volatile Data Collection – Windows- In-depth data collection – Windows- Storing collected data – Windows-Creating response toolkit – Unix- Volatile Data Collection – Unix- In-depth data collection – Unix-Storing collected data – Unix.

UNIT II **6**

Introduction to ACPO Principles- ACPO Principles of Computer Based Evidence- Introduction to computer Storage Formats- Understanding Storage Formats for Digital Evidence-Forensic Duplication-Forensic Duplication tools-Forensic Duplicate creation of HDD- Qualified Forensic Duplicate creation-Restored Image-Mirror Image- Forensic Duplication Tool Requirements-Creating a Forensic Duplicate of a Hard Drive- Evidence Handling-Types of Evidence-Challenges in Evidence Handling- Overview of Evidence Handling Procedure- Evidence Handling Procedure-Evidence Handling reports.

UNIT III **6**

Introduction to File System Analysis- What is a File System?- Five Data Categories- FAT Concepts- FAT Analysis- FAT - The Big Picture- Introduction to NTFS- Files in NTFS- MFT Concepts- MFT Attribute Concepts- Other MFT Attribute Concepts- Indexes in NTFS- NTFS Analysis - File System Category-NTFS Analysis - Content Category- NTFS Analysis - Metadata Category- NTFS Analysis - File Name Category- NTFS Analysis - Application Category- NTFS - The Big Picture.

UNIT IV **6**

Introduction to Investigating Systems- Investigating Windows Systems- Where Evidence resides on Windows Systems -Conducting a Windows Investigation I-Conducting a Windows Investigation II-File Auditing-Theft of Information-Handling the departing employee-Investigating Unix Systems-Overview of steps - Unix Investigation-Reviewing pertinent logs-Performing keyword searches-Reviewing relevant files-Identifying unauthorized user accounts/groups-Identifying rogue processes-Checking for unauthorized access points-Analyzing trust relationships-Detecting loadable kernel modules

UNIT V **6**

Investigating Hacker Tools-What are the goals of tool analysis?- How are files compiled?- Static Analysis of Hacker Tools I-Static Analysis of Hacker Tools II-Dynamic Analysis of Hacker Tools I-Dynamic Analysis of Hacker Tools II-Evaluating Computer Forensics Tools-Types of Forensic Tools-Tasks performed by Forensic Tools-Tool comparisons-Computer Forensics Software Tools-Computer Forensics Hardware Tools-Validating and Testing Computer Forensics Software-Introduction to Forensic Report Writing-Understanding the Importance of Reports-Guidelines for Writing Reports-A Template for Computer Forensics Reports

Total Theory Hours: 30 Periods

LABORATORY EXPERIMENTS:

1. Mirroring the disk and convert into Hashcodes.
2. Analysis of Disk Imaging.
3. Analysis of Sim Card Imaging.
4. Analysis of online windows Forensics.
5. Analysis of Cell Phone Towers.

Total Lab hours: 15 Periods
Total Hours: 45 Periods

REFERENCE BOOK(S):

1. KevinMandia, ChrisProsise,"IncidentResponseandcomputerforensics", TataMcGrawHill, 2006.
2. Bill Nelson,Amelia Philips and Christopher Steuart, "Guide to computer forensics and investigations",coursetechnology,CengageLearning;4thedition,ISBN:1-435-49883-6,2009.
3. EoghanCasey,"HandbookComputerCrimeInvestigation'sForensicToolsandTechnology",Academic Press, 1st Edition,2001.
4. Brian Carrier, "File System Forensic Analysis", Addison-Wesley Professional; 1st edition 2005, ISBN-13:978-0321268174

WEB RESOURCE(S):

1. https://www.pdfdrive.com/incident-response-computer-forensics-3rd-edition-e60282743.html
2. https://www.profajaypashankar.com/wp-content/uploads/2018/12/Guide-to-Computer-Forensics-and-Investigations-1.pdf
3. https://repo.zenk-security.com/Forensic/File%20System%20Forensic%20Analysis.pdf
4. https://www.cert-in.org.in/Downloader?pageid=5&type=2&fileName=CIPS-2010-0164.pdf
5. https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html#:~:text=There%20are%20four%20phases%20involved,on%20Introduction%20to%20Digital%20Forensics).
6. http://ocw.ump.edu.my/pluginfile.php/13418/mod_resource/content/1/Ch5-1-%20Storage%20Formats%20for%20Digital%20Evidence.pdf

COURSE OUTCOME(S):

CO1: Acquire the knowledge on basics of procedures for identification, preservation of electronic evidence.
CO2: Acquire the ability to identify the purpose and usage of various forensic tools.
CO3: Understand how scientific evidence collection/extraction during investigation.
CO4: Appreciate the concepts of file systems and its importance in forensic science.
CO5: Apply the knowledge of windows and Linux investigation procedures.
CO6: Acquire the knowledge on forensic report writing guidelines and principles

PO Vs CO MAPPING:

CO No	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	3	2		2								
2	2	2		2								
3	2	3		3								
4	2	2	1	2								
5	2	3		3								

1→Low 2→Medium 3→High

Elective Courses

21CS7S01 **CLOUD SECURITY** **L T P C**

3 0 0 3

Course Objectives:

- To understand the Cloud Architecture with concepts
- Gain knowledge on cloud security
- Acquire knowledge on Cloud Platform and Infrastructure Security
- To understand Cloud Application Security
- Gain knowledge on the Evaluating cloud security and Security operations activities.

PRE-REQUISITE:

- **Nil**

UNIT I **9**

Cloud Architecture: Cloud Computing concepts, Reference architecture, Security Concerns, Risk issues and legal aspects, Security requirements, Security patterns and architecture elements, Cloud Security architecture, ISO security standards.

UNIT II **9**

Cloud Data Security: Overview, Lifecycle, Storage architectures, Security strategies, Data discovery and classification techniques, Data encryption: Application and limits, Sensitive data categorization, Data rights management, policies, Events-audit, trace and account.

UNIT III **9**

Cloud Platform and Infrastructure Security: Components, Security controls, Disaster recovery and Business continuity, Security criteria for building an internal cloud and selecting an external cloud provider.

UNIT IV **9**

Cloud Application Security: Training and awareness, Software assurance and validation, Secure software, secure SDLC process, Cloud application architecture, Identity and access management.

UNIT V **9**

Securing the cloud: Evaluating cloud security – checklist, metrics, security monitoring, best practices, Operating a Cloud – From architecture to secure operations, Security operations activities.

Total: 45 Periods

REFERENCE BOOK(S):

1. Daniel Carter, "CCSP Certified Cloud Security Professional All-in-One Exam Guide", First edition, McGraw-Hill Education, 2017.
2. Vic (J.R.) Winkler, "Securing the Cloud: Cloud Computer Security Techniques and Tactics", Syngress/Elsevier, First edition, 2011.
3. Brian T. O'Hara, Ben Malisow, "CCSP (ISC)2 Certified Cloud Security Professional Official Study Guide", 1st edition, Wiley, 2017.
4. RajkumarBuyya, Christian Vecchiola, S.ThamaraiSelvi, "Mastering cloud computing", Morgan Kaufman, 2013.
5. Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing", 2011.
6. ObyVelte, Anthony Velte, Robert Elsenpeter, "Cloud Computing, A Practical Approach" McGraw-Hill Osborne Media; 1 edition [ISBN: 0071626948], 2009.

WEB RESOURCE(S):

1. https://www.tutorialspoint.com/cloud_computing/cloud_computing_architecture.html
2. https://www.slideshare.net/MohammedFazuluddin/cloud-computing-and-data-security
3. https://slideplayer.com/slide/7287038/
4. https://www.tutorialspoint.com/cloud_computing/cloud_computing_security.html
5. https://www.slideshare.net/AmyNicewick/cloud-application-security-ccsp-domain-4

COURSE OUTCOME(S):

CO1: Describe the design requirements of secure cloud architecture

CO2: Utilize appropriate techniques to enable cloud data security for the given scenario.

CO3: Adapt the security criteria's recommended to build the cloud infrastructure.

CO4: Practice the secure software engineering principles for developing cloud applications.

CO5: Examine the security concerns and operations involved in the cloud

PO Vs CO MAPPING:

CO No	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	2	1										
2	3	2	2		2	2			2		2	
3	3	2	2		2	2			2		2	
4	3	2	2		2	2			2		2	
5	3	3	2	1	2	2	2	2	2	2	2	

1→Low 2→Medium 3→High

21CS7S02 DATABASE SECURITY L T P C

3 0 0 3

Course Objectives:

- Demonstrate understanding of Fundamentals of Security in database technology with its security architecture in modern computer systems in a typical enterprise
- Formulate a working definition of database security and administration and Identify contemporary practices of operating system security.
- To identify risks and vulnerabilities in operating systems from a database perspective
- Demonstrate the knowledge and skills for administration of user, profiles, password policies, privileges and roles.
- Manage database security Model on application level and Conduct database auditing for security and reliability
- Implement typical security projects on enterprise systems

Pre-requisite Courses:

- Nil

UNIT I **9**

Importance of Data,Identity Theft- Levels of data security- Authorization in databases- ACL Application Vulnerabilities- Database security issues- Access to key fields,Access to Activities: surrogate information- Problems with data extraction- Access control in SQL- Discretionary security in SQL,Schema level- Authentication, Table level- SQL system tables, Mandatory security in SQL- Data protection

UNIT II **9**

Installing a typical database product- Security architecture: Database Management Systems- Information Security Architecture- Database Security, Basics of Security in distributed databases- Asset Types and value-Security Methods- Operating system security principles- Security Environment- Components- Authentication Methods- User Administration- Password Policies- Vulnerabilities- E-mail Security

UNIT III **9**

Introduction-Authentication-Creating Users- SQL Server User- Removing,Modifying Users- Default, Remote Users- Database Links-Linked Servers- Remote Servers-Practices for Administrators and Managers- Best Practices Profiles- Password Policies- Introduction-Defining and Using Profiles- Designing and Implementing Password Policies- Granting and Revoking User Privileges- Creating, Assigning and Revoking User Roles-Best Practices

UNIT IV **9**

Database Application Security Models: Introduction- Types of Users- Security Models- Application Types-Application Security Models- Data Encryption.Excessive privileges, SQL Injections- Countermeasures of Malware, Countermeasures of Weak Audit Trail- DB Vulnerabilities and Misconfiguration- Countermeasures of Denial of Service,Stolen Database Backups- CONTROL METHODS: Access Control,Access control models for XML databases, Inference Policy User Identification,Authentication, Accountability,Password Crptography

UNIT V **9**

Virtual Private Databases:Introduction-Overview- Implementation of VPD using Views- Application Context in Oracle- Implementing Oracle VPD- Viewing VPD Policies and Application contexts using Data Dictionary- Policy Manager Implementing Row and Column level Security with SQL Server- Auditing Database Activities: Creating DLL Triggers with Oracle- Auditing Server Activity with SQL SLO-2 Server 2000- Using Oracle Database Activities- Security Project Case study- Security and Auditing Project Case Study Data Protection SLO-2 and the IoT

Total: 45 Periods

REFERENCE BOOK(S):

1. Alfred Basta ,Melissa Zgola and Dana Bullaboy “Database Security” 1st Edition Cingage ,2012 (Unit 1 toIII)
2. Hassan A. Afyouni, “Database Security and Auditing”, Third Edition, Cengage Learning,2009.(UNIT III to V)

3. Michael Gertz and SushilJajodia (Editors) ,*Handbook of Database Security: Applications and Trends* , ISBN-10: 0387485325. Springer, 2007

WEB RESOURCE(S):

1. https://www.scribd.com/document/457977203/Alfred-Basta-Melissa-Zgola-Database-Security-Cengage-Learning-2011-pdf
2. https://www.cs.uct.ac.za/mit_notes/database/pdfs/chp12.pdf
3. http://aircconline.com/ijist/V6N2/6216ijist18.pdf (UnitIV)

COURSE OUTCOME(S):

- Students are able to identify fundamentals of data , security of data and security issues
- Students are obtaining knowledge about architecture of data base security and Operating System Security
- Develop and implement a security plan for an enterprise level database (password policies, auditing policies, user privileges, profile, and roles).
- Students are able to design and implement access control rules to assign privileges and protect data in databases.
- Identify some of the factors driving the need for Database security and classify particular examples of attacks
- Students implement database auditing and Virtual Private Database to protect data in databases

PO Vs CO MAPPING:

CO No	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	3	2		2								
2	3	2		2								
3	1	2	3	2								
4	1	2	2	2								
5		3		3								
6			3									

1→Low 2→Medium 3→High

21CS7S03 MOBILE AND WIRELESS SECURITY L T P C

3 0 0 3

Course Objectives:

- Gain knowledge on the Introduction to wireless technologies
- Understand the purpose and usage of wireless threats.
- Gain knowledge on Mobile networks security and Wireless transport layer security
- Acquire knowledge on Bluetooth and Wifi security.
- Understand the case studies in wireless networks.

PRE-REQUISITE:

- **Nil**

UNIT I **9**

Mobile & Wireless technologies: Introduction to wireless technologies - Mobile cellular networks - Personal Area Networks -Transmission Media – WLAN standards, controllers - Securing WLAN - Countermeasures - Wired Equivalence Protocol (WEP).

UNIT II **9**

Wireless threats: Kinds of security breaches - Eavesdropping - Communication Jamming - RF interference - Covert wireless channels - DOS attack – Spoofing - Theft of services - Traffic Analysis-Cryptographic threats - Wireless security Standards.

UNIT III **9**

Mobile networks security: Wireless Device security issues - CDPD security (Cellular Digital Packet Data)-GPRS security (General Packet Radio Service) - GSM (Global System for Mobile Communication) security – IP security - 3G / 4G security.

Wireless transport layer security: Secure Socket Layer - Wireless Transport Layer Security - WAP Security Architecture - WAP Gateway - Wireless Intrusion Detection and Prevention Systems (WIDS/WIPS).

UNIT IV **9**

Bluetooth & WiFi security: Basic specifications - Pico nets – Scatter nets - Bluetooth security architecture – Security at the baseband layer and link layer – Frequency hopping – Security manager – Authentication – Encryption - WiFi Hot spot architecture - Wireless honeypots - Security in IEEE 802.11. **Wireless Sensor Network Security** Attacks on wireless sensor network

and Preventive mechanisms: authentication and traffic analysis, Case study: centralized and passive intruder detection

UNIT V **9**

Case studies: Case study 1 – Public safety wireless networks, Case study 2 – Satellite communications systems , Case study 3 – Wide Area Wireless Data Services (CDPD, GPRS, etc.), Case study 4 – Wireless LANs (802.11, etc.), Case study 5 – Wireless Metropolitan Area Networks (e.g., 802.16)

Total: 45 Periods

REFERENCE BOOK(S):

1. Wireless and Mobile Network Security-Security basics, Security in On-the-shelf and emerging technologies, Hakima Chaouchi, Maryline Maknavicius, ISBN: 9781848211179, 2010.
2. Wireless Security-Models, Threats and Solutions, Nichols and Lekka, Tata McGraw – Hill, New Delhi, 2006.
3. Wireless Security, Merritt Maxim and David Pollino, Osborne/McGraw Hill, New Delhi, 2005.
4. Mobile and Wireless Network Security and Privacy, Springer, ISBN: 0387710574, edition 2007.
5. Wireless Network Security: Theories and Applications, Springer, ISBN: 978-3642365102, 2013

WEB RESOURCE(S):

1. https://www.wiley.com/en-us/Wireless+and+Mobile+Network+Security-p-9781848211179
2. https://www.coursehero.com/file/p330ide/5-Nichols-and-Lekka-Wireless-Security-Models-Threats-and-Solutions-Tata-McGraw
3. https://archive.org/details/wirelesssecurity0000maxi/page/n11/mode/2up

COURSE OUTCOME(S):

CO1: Explain various wireless technologies, wireless network standards and their threats

CO2: Identify how hackers and auditors alike test wireless networks for vulnerabilities such as rogue access points, denial of service (DoS) attacks and client-side threats.

CO3: Explain the mobile data network standards and its challenges.

CO4: Discover the vulnerabilities and mis - configurations at wireless transport layer.

CO5: Show how an attacker might attempt to subvert and bypass Wireless security measures in Bluetooth and WiFi.

CO6: Demonstrate various hacking and vulnerability assessment tools to assess the security of wireless and sensor networks, including cracking WEP and WPA security

PO Vs CO MAPPING:

CO No	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	2	1										
2	2	1										
3	2	1										
4	2	1		1								
5	2	2	1	1								
6	3	2	2	1	1			1	2	1	1	

1→Low 2→Medium 3→High