Semester- III

Ethical Hacking			
Course Code	**MMCH311A**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	3:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:

- To develop a comprehensive understanding of ethical hacking principles, methodologies, and tools, and recognize the significance of ethical and legal considerations in conducting security assessments.
- To acquire hands-on proficiency in executing penetration tests, vulnerability assessments ,and Ethical hacking techniques across various system components, networks, and applications.
- To demonstratetheabilitytoidentify,assess,andprioritizevulnerabilitiesindiversecomputing environmentsusingbothmanualandautomatedmethods,andeffectivelycommunicatethese findings to stakeholders.
- To develop a strategic mindset towards cyber security by acquiring knowledge of common attack Vectors,learningtosimulatereal-worldattacks,andimplementingpreventivemeasuresto secure systems,Networks and web applications.

Module-1

Introduction to Ethical Hacking

Introduction to ethical hacking and its importance, Legal and ethical considerations in ethical hacking, Differentiating between black hat, white hat, and grey hat hacking, Basic cyber security concepts and terminology, Overview of penetration testing methodologies

Textbook:1 Chapter1 Textbook:2 Chapter1,2

Module-2

Foot printing and Information Gathering

Passive and active information gathering techniques, Who is lookup, DNS enumeration, and social engineering, Tools and methodologies for foot printing, Google hacking and OSINT (Open Source Intelligence) techniques

Textbook:1 Chapter3

Module-3

Scanning and Enumeration: Port scanning techniques: SYN,TCP,UDP scans; Service enumeration and version detection; NetBIOS, SNMP, and SMTP enumeration; Vulnerability scanning and assessment

Textbook:1 Chapter 3,4, 5

Module-4

System Hacking and Exploitation

Passwordcrackingtechniquesandtools;Privilegeescalationandmaintainingaccess;Malware types andcountermeasures;Exploitingcommonvulnerabilities(e.g.,bufferoverflow,SQLinjection)

Textbook:1 Chapter 7, 9, 10

Module-5

Web Application and Network Security

Common web vulnerabilities: SQL injection, XSS, CSRF; Web application penetration testing methodology; Network sniffing and spoofing; Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

Textbook:1 Chapter6, 12 Textbook:1 Chapter1

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Two Unit Tests each of **25 Marks**
2. Two assignments each of **25 Marks** or **one Skill Development Activity of 50 marks** to attain the COs and POs

The sum of two tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

1. The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
2. The question paper will have ten full questions carrying equal marks.
3. Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
4. Each full question will have a sub-question covering all the topics under a module.
5. The students will have to answer five full questions, selecting one full question from each modul

Suggested Learning Resources:Books

Text Books

1	RafayBaloch,EthicalHackingandPenetrationTestingGuide,CRCPress,2015,ISBN978-1-4822-3161-8(Paperback)
2	HarperAllen,GrayHatHacking:TheEthicalHackersHandBook,3rdEdition,McGrawHill,2011.
3	JayBeale,AndrewR.Baker,JoelEsler,SnortIntrusionDetectionandPreventionToolkit,Syngress Publishing,Inc,2007,ISBN-13:978-1-59749-099-3

Reference Books

1	WilliamStallings,NetworkSecurityEssentials:ApplicationsandStandards,PearsonEducation Limited2017,ISBN13:978-1-292-15485-5
2	PatrickEngebretson,TheBasicsofHackingandPenetrationTesting,SyngressPublishing,2013, ISBN978-0-12-411644-3

E- Resources (NPTEL/ SWAYAM. Any Other)-mention links

Nmap-Official Documentation :https://nmap.org/book/

National Vulnerability Database(NVD):https://nvd.nist.gov/

Course Outcomes(COs)

At the end of the course, the student will be able to		**Learning Level**
CO1	**Explain** the core concepts, principles and legal Considerations of ethical hacking.	L2
CO2	**Make us of** different tools and techniques for information gathering, scanning and enumeration	L3
CO3	**Apply** tools and techniques for exploiting vulnerabilities, Network sniffing, web application hacking, system hacking, Escalating privileges, etc.	L3
CO4	**Analyze** the results of IDS/IPS, ethical hacking and penetration testing tasks	L4

Mapping of COS and POs

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**
CO1	1					2		
CO2	2				2	3		
CO3	3				2	3		
CO4	3				3	2	3	

Semester-III

<table>
<tr><td colspan="4" align="center">Cyber Security</td></tr>
<tr><td>Course Code</td><td align="center">MMCH311B</td><td>CIE Marks</td><td align="center">50</td></tr>
<tr><td>Teaching Hours/Week (L:P:SDA)</td><td align="center">3:0:0</td><td>SEE Marks</td><td align="center">50</td></tr>
<tr><td>Total Hours of Pedagogy</td><td align="center">40</td><td>Total Marks</td><td align="center">100</td></tr>
<tr><td>Credits</td><td align="center">03</td><td>Exam Hours</td><td align="center">03</td></tr>
<tr><td colspan="4">Course Learning objectives:
To learn cybercrime and cyber law.
To understand the cyber-attacks and tools for mitigating them.
To understand information gathering.
To learn how to detect a cyber-attack.
To learn how to prevent a cyber-attack.</td></tr>
<tr><td colspan="4" align="center">Module-1</td></tr>
<tr><td colspan="4">INTRODUCTION Cyber Security – History of Internet – Impact of Internet – CIA Triad; Reason for Cyber Crime – Need for Cyber Security – History of Cyber Crime; Cybercriminals – Classification of Cybercrimes – A Global Perspective on Cyber Crimes; Cyber Laws – The Indian IT Act – Cybercrime and Punishment.</td></tr>
<tr><td colspan="4" align="center">Module-2</td></tr>
<tr><td colspan="4">ATTACKS AND COUNTER MEASURES OSWAP; Malicious Attack Threats and Vulnerabilities: Scope of Cyber-Attacks – Security Breach – Types of Malicious Attacks – Malicious Software – Common Attack Vectors – Social engineering Attack – Wireless Network Attack – Web Application Attack – Attack Tools – Counter measures.</td></tr>
<tr><td colspan="4" align="center">Module-3</td></tr>
<tr><td colspan="4">RECONNAISSANCE Harvester – Who is – Netcraft – Host – Extracting Information from DNS – Extracting Information from E-mail Servers – Social Engineering Reconnaissance; Scanning – Port Scanning – Network Scanning and Vulnerability Scanning – Scanning Methodology – Ping Sweer Techniques – Nmap Command Switches.</td></tr>
<tr><td colspan="4" align="center">Module-4</td></tr>
<tr><td colspan="4">INTRUSION DETECTION Host -Based Intrusion Detection – Network -Based Intrusion Detection – Distributed or Hybrid Intrusion Detection – Intrusion Detection Exchange Format – Honeypots – Example System Snort.</td></tr>
<tr><td colspan="4" align="center">Module-5</td></tr>
<tr><td colspan="4">INTRUSION PREVENTION Firewalls and Intrusion Prevention Systems: Need for Firewalls – Firewall Characteristics and Access Policy – Types of Firewalls – Firewall Basing – Firewall Location and Configurations –Intrusion Prevention Systems – Example Unified Threat Management Products.</td></tr>
</table>

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Two Unit Tests each of **25 Marks**
2. Two assignments each of **25 Marks** or **one Skill Development Activity of 50 marks** to attain the COs and POs

The sum of two tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

1. The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
2. The question paper will have ten full questions carrying equal marks.
3. Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
4. Each full question will have a sub-question covering all the topics under a module.
5. The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:

Books

TEXT BOOKS:

1. Patrick Engebretson, "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made easy", Elsevier, 2011. (Unit-3)
2. William Stallings, Lawrie Brown, "Computer Security Principles and Practice", Third Edition, Pearson Education, 2015. (Unit-4 & 5)
3. Anand Shinde, "Introduction to Cyber Security Guide to the World of Cyber Security", Notion Press, 2021. (Unit-1 &2)

REFERENCE BOOKS

1. David Kim, Michael G. Solomon, "Fundamentals of Information Systems Security", Jones & Bartlett Learning Publishers, 2013.
2. Nina Godbole, Sunit Belapure, "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley Publishers, 2011.

Course outcome (Course Skill Set)

At the end of the course the student will be able to :

Sl. No.	Description	Blooms Level
CO1	Explain the basics of cyber security, cybercrime and cyber law	
CO2	Classify various types of attacks and learn the tools to launch the attacks	
CO3	Apply various tools to perform information gathering	
CO4	Apply intrusion techniques to detect intrusion	
CO5	Apply intrusion prevention techniques to prevent intrusion	

Mapping of COS and Pos

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1		1						
CO2		2		3				
CO3	2	2			3			
CO4	2	2			3	3		
CO5		1		2			3	

Semester- III

Cryptography and Network Security			
Course Code	**MMCH311C**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	3:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:

- To make the student learn different encryption techniques along with hash functions, MAC, digital signatures and their use in various protocols for network security and system security.

Module-1

INTRODUCTION: Computer Security Concepts, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, A Model for Network Security. CLASSICAL ENCRYPTION TECHNIQUES: Symmetric Cipher Model, Substitution Techniques, Transposition Techniques, Steganography.

Module-2

BLOCK CIPHERS AND THE DATA ENCRYPTION STANDARD: Block Cipher Principles, The Data Encryption Standard (DES), A DES Example, The Strength of DES, Differential and Linear Cryptanalysis, Block Cipher Design Principles. BLOCK CIPHER OPERATION: Multiple Encryption and Triple DES, Electronic Codebook Mode, Cipher Block Chaining Mode, Cipher Feedback Mode, Output Feedback Mode, Counter Mode. STREAM CIPHERS : Stream ciphers,RC4 Ciphers, RC4.

Module-3

NUMBER THEORY-: Divisibility and the Division Algorithm, The Euclidean Algorithm, Modular Arithmetic, Prime Numbers, Fermat"s and Euler's Theorems, Testing for Primality, The Chinese Remainder Theorem, and Discrete Logarithms. PUBLIC-KEY CRYPTOGRAPHY, RSA AND OTHER PUBLIC-KEY CRYPTOSYSTEMS: Principles of Public-Key Cryptosystems, The RSA Algorithm, DiffieHellman Key Exchange, ElGamal Cryptosystem.

Module-4

CRYPTOGRAPHIC HASH FUNCTIONS: Applications of Cryptographic Hash Function, Two Simple Hash Functions, Requirements and Security, Hash Functions Based on Cipher Block Chaining, Secure Hash Algorithm (SHA). MESSAGE AUTHENTICATION CODES: Message Authentication Requirements, Message Authentication Functions, Message Authentication Codes, Security of MACs, MACs Based on Hash Functions (HMAC).

Module-5

DIGITAL SIGNATURES- Digital Signatures, ElGamal Digital Signature Scheme, Schnorr Digital Signature Scheme, Digital Signature Standard (DSS). KEY MANAGEMENT AND ISTRIBUTION: Symmetric Key Distribution Using Symmetric Encryption, Symmetric Key Distribution Using Asymmetric Encryption, Distribution of Public Keys, X.509 Certificates, Public Key Infrastructure.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Two Unit Tests each of **25 Marks**
2. Two assignments each of **25 Marks** or **one Skill Development Activity of 50 marks** to attain the COs and POs

The sum of two tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

1. The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
2. The question paper will have ten full questions carrying equal marks.
3. Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
4. Each full question will have a sub-question covering all the topics under a module.
5. The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:

Text Books:

1. William Stallings: Cryptography and Network Security- Principles And Practice, 5th Edition, Pearson/PHI, 2011.

Reference books:

1. William Stallings, "Network Security Essentials (Applications and Standards)", 4th Edition, Pearson Education. , 2012
2. Charlie Kaufman, Radia Perlman and Mike Speciner: "Network Security – Private Communication in a Public World", 2nd Edition, Pearson/PHI, 2002.
3. Eric Maiwald: "Fundamentals of Network Security", 1st Edition, Dreamtech Press, 2003.
4. Whitman: "Principles of Information Security", 3rd Edition, Thomson, 2009.
5. Robert Bragg, Mark Rhodes: "Network Security: The complete reference", 1st Edition, TMH, 2004.
6. Buchmann: "Introduction to Cryptography", 2nd Edition, Springer, 2004.

Web links and Video Lectures (e-Resources):

- http://www.nptel.iitm.ac.in/courses/106105031/.
- https://www.youtube.com/playlist?list=PLBlnK6fEyqRgJU3EsOYDTW7m6SUmW6kII&utm_source=chatgpt.com
- https://www.youtube.com/playlist?list=PL71FE85723FD414D7
- https://www.youtube.com/playlist?list=PL_LGG4Jw4MdFPrMZg-otwrRPPAoXT-vgO
- https://onlinecourses.nptel.ac.in/noc20_cs21/preview?utm_source=chatgpt.com

Skill Development Activities Suggested

- Implement Caesar Cipher and Vigenère Cipher using Python.
- Implement DES and Triple DES encryption using a programming language.
- Write code for Euclidean algorithm, Modular inverse, and Chinese Remainder Theorem.
- Case study: Discuss a real-world cyberattack prevented using public-key crypto.
- Build a simple login system with hashed passwords.
- Implement a digital signature using ElGamal or RSA.

Course outcome (Course Skill Set)

At the end of the course the student will be able to:

Sl. No.	Description	Blooms Level
CO1	Analyze and design classical encryption techniques and block ciphers	L2
CO2	Understand and analyze data encryption standard.	L2
CO3	Understand and analyze public-key cryptography, RSA and other public-key cryptosystems	L2
CO4	Understand key management and distribution schemes and design User Authentication, such as Diffie-Hellman Key Exchange, ElGamal Cryptosystem, etc	L2
CO5	Apply intrusion prevention techniques to prevent intrusion	L2

Mapping of COS and Pos

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1		1			2			
CO2	2				1			
CO3		2				3		
CO4	1		2					
CO5		1		2				3

Semester- III

Blockchain Technologies			
Course Code	**MMCH311D**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	3:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:

- Demonstrate the basics of Block chain concepts using modern tools/technologies.
- Illustrate the role of block chain applications in different domains including cyber security.
- EvaluatetheusageofBlockchainimplementation/featuresforthegivenproblem.
- Exemplify the usage of bit coins and its impact on the economy.
- Analyzetheapplicationofspecificblockchainarchitectureforagivenproblem

Module-1

Introduction to Blockchain,How Blockchain works, Blockchain vs Bitcoin, Practical applications, public and Private key basics, pros and cons of Blockchain,Myths about Bitcoin.

Module-2

Block chain: Architecture, versions, variants, use cases, Life use cases of block chain, Block chain vs shared Database,Introduction to crypto currencies, Types, Applications.Ciphers, RC4.

Module-3

Concept of Double Spending, Hashing, Mining, Proof of work. Introduction to Merkel tree, Privacy ,payment verification , Resolving Conflicts , Creation of Blocks

Module-4

Introduction to Bitcoin, key concepts of Bitcoin, Merits and De Merits Fork and Segwits, Sending and Receiving bitcoins, choosing bitcoin wallet, Converting Bitcoins to Fiat Currency.

Module-5

Introduction to Ethereum, Advantages and Disadvantages, Ethereum vs Bitcoin, Introduction to Smart contracts, usage, application, working principle, Law and Regulations. Case Study.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Two Unit Tests each of **25 Marks**
2. Two assignments each of **25 Marks** or **one Skill Development Activity of 50 marks** to attain the COs and POs

The sum of two tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

1. The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
2. The question paper will have ten full questions carrying equal marks.
3. Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
4. Each full question will have a sub-question covering all the topics under a module.
5. The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:

- Beginning Block chain: A Beginner's Guide to Building Blockchain Solutions by ArshdeepBikramaditya Signal,Gautam Dhameja (Priyansu Sekhar Panda., A Press.) 2018
- Block chain Applications: A Hands-On Approach by Bahga, Vijay Madisetti ,2017
- Block chain by Melanie Swan, O Reilly 2015

Reference Books

- Bitcoin and Cryptocurrency Technologies by Aravind Narayan. Joseph Bonneau, princton
- Bitcoin and Blockchain Basics: A non-technical introduction for beginners by Arthu.T Books.

Web links and Video Lectures (e-Resources):

- https://youtu.be/mzPoUjQC4WU

Skill Development Activities Suggested

- Create a comparative chart: Blockchain vs Bitcoin vs Traditional Databases.
- Develop a flowchart showing how a cryptocurrency transaction flows through a blockchain.
- Simulate the proof-of-work process using hash functions (SHA256) in Python.
- Create a bitcoin wallet using a mobile app or online simulator (no real money involved).

Course outcome (Course Skill Set)
At the end of the course the student will be able to:

Sl. No.	Description	Blooms Level
CO1	Demonstrate the basics of Block chain concepts using modern tools/technologies.	L2
CO2	Analyze the role of block chain applications in different domains including cyber security.	L3
CO3	Evaluate the usage of Block chain implementation/features for the given problem.	L2
CO4	Exemplify the usage of bitcoins and its impact on the economy	L2
CO5	Analyze the application of specific block chain architecture for a given problem	L2

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1		1			1			
CO2	1		2					
CO3		2				2		
CO4				2	3			
CO5			3			3		

Semester- III

Database & Web Application Security			
Course Code	**MMCH311E**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	3:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:

- To understand the fundamentals of database security concepts, Identify key security threats and vulnerabilities.
- To examine security mechanisms and best practices for database protection Design and implement security solutions.
- To identify and analyze vulnerabilities in web applications and databases.
- To design secure web applications
- To evaluate tools and techniques for detecting and mitigating security breaches

Module-1

SUPPORTING TECHNOLOGIES FOR DATABASE AND APPLICATIONS SECURITY: Data Management Technologies, Information Security, Information Management Technologies.

Module-2

DISCRETIONARY SECURITY FOR DATABASE SYSTEMS: Security Policies, Policy Enforcement and Related Issues.

Module-3

MANDATORY SECURITY FOR DATABASE SYSTEMS: Historical Developments, Design Principles.

Module-4

MULTILEVEL SECURE RELATIONAL DATABASE SYSTEMS: Multilevel Relational Data Models, Security Impact on Database Functions, Prototypes and Products.

Module-5

THE INFERENCE PROBLEM: A Perspective of the Inference Problem, Security-Constraint Processing for Inference Control, Conceptual Structures for Inference Control

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Two Unit Tests each of **25 Marks**
2. Two assignments each of **25 Marks** or **oneSkill Development Activity of 50 marks** to attain the COs and POs

The sum of two tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

1. The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
2. The question paper will have ten full questions carrying equal marks.
3. Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
4. Each full question will have a sub-question covering all the topics under a module.
5. The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:

TEXT BOOKS:

1. BhavaniThuraisingham, "Database and Applications Security", Integrating Information Security and Data Management, Auerbach Publications, 2005.

REFERENCES:

1. Michael Gertz and SushilJajodia, "Handbook of Database Security— Applications andTrends", Springer, 2008.
2. Bryan and Vincent, "Web Application Security, A Beginners Guide", McGraw-Hill, 2011
3. Alfred Basta, Melissa Zgola, "Database Security", Course Technology, 2012.

Web links and Video Lectures (e-Resources):

- https://www.scribd.com/document/450222788/1-2012-Web-Application-Security-a-Beginer-Guide

Skill Development Activities Suggested

- Use OWASP Juice Shop or DVWA (Damn Vulnerable Web Application) to identify and exploit vulnerabilities like SQL Injection, XSS, CSRF.
- Students rewrite vulnerable code snippets using secure practices (input validation, sanitization, etc.).

Course outcome (Course Skill Set)

At the end of the course the student will be able to:

Sl. No.	Description	Blooms Level
CO1	Describe core concepts of database and web application security, including data confidentiality, integrity, and access control.	L1
CO2	Identify and explain common vulnerabilities in web applications and databases.	L2
CO3	Apply appropriate security mechanisms (encryption, authentication, access control) to protect databases and web applications.	L2
CO4	Develop secure web applications using industry best practices and secure coding techniques.	L3
CO5	Use tools and techniques to analyze, test, and mitigate real-world security threats and attacks.	L3

Mapping of COS and Pos

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	**1**							
CO2		**2**						**3**
CO3						**3**		
CO4				**2**				
CO5			**3**					

Semester- III

Mobile and Wireless Security			
Course Code	**MMCH311F**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	3:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:

- Understand mobile and wireless communication fundamentals.
- Identify key security threats and vulnerabilities.
- Analyze security mechanisms in mobile and wireless systems.
- Design and implement security solutions
- Explore emerging trends and research areas

Module-1

Security Issues in Mobile Communication: Mobile Communication History, Security – Wired Vs Wireless, Security Issues in Wireless and Mobile Communications, Security Requirements in Wireless and Mobile Communications, Security for Mobile Applications, Advantages and Disadvantages of Application – level Security.

Module-2

Security of Device, Network, and Server Levels: Mobile Devices Security Requirements, Mobile Wireless network level Security, Server Level Security. Application-Level Security in Wireless Networks: Application of WLANs, Wireless Threats, Some Vulnerabilities and Attach Methods over WLANs, Security for 1G Wi-Fi Applications, Security for 2G Wi-Fi Applications, Recent Security Schemes for Wi-Fi Applications

Module-3

Application-Level Security in Cellular Networks: Generations of Cellular Networks, Security Issues and attacks in cellular networks, GSM Security for applications, GPRS Security for applications, UMTS security for applications, 3G security for applications, Some of Security and authentication Solutions.

Module-4

Application-Level Security in MANETs: MANETs, Some applications of MANETs, MANET Features, Security Challenges in MANETs, Security Attacks on MANETs, External Threats for MANET applications, Internal threats for MANET Applications, Some of the Security Solutions. Ubiquitous Computing, Need for Novel Security Schemes for UC, Security Challenges for UC, and Security Attacks on UC networks, Some of the security solutions for UC.

Module-5

Security for Mobile Commerce Application: M-commerce Initiatives, Security Challenges in Mobile E-commerce, Types of Attacks on Mobile E-commerce, A Secure M-commerce Model Based on Wireless Local Area Network, Some of M-Commerce Security Solutions

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Two Unit Tests each of **25 Marks**
2. Two assignments each of **25 Marks** or **one Skill Development Activity of 50 marks** to attain the COs and POs

The sum of two tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

1. The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
2. The question paper will have ten full questions carrying equal marks.
3. Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
4. Each full question will have a sub-question covering all the topics under a module.
5. The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:

TEXT BOOKS:

1. Pallapa Venkataram, Satish Babu: "Wireless and Mobile Network Security", 1st Edition, Tata McGraw Hill,2010.
2. Frank Adelstein, K.S.Gupta : "Fundamentals of Mobile and Pervasive Computing", 1st Edition, Tata McGraw Hill 2005**.**

REFERENCES:

1. Randall k. Nichols, Panos C. Lekkas: "Wireless Security Models, Threats and Solutions", 1st Edition, Tata McGraw Hill, 2006.
2. Bruce Potter and Bob Fleck: "802.11 Security," 1st Edition, SPD O'REILLY 2005.
3. James Kempf: "Guide to Wireless Network Security, Springer. Wireless Internet Security – Architecture and Protocols", 1st Edition, Cambridge University Press, 2008

Web links and Video Lectures (e-Resources):

- https://dokumen.pub/qdownload/wireless-and-mobile-network-security-9780070700246-0070700249.html

Skill Development Activities Suggested

- Programming Assignment-1: Implementation of important concepts of data manipulation using NumPy and Pandas (Python
- Programming Assignment-2: Implementation of simple Machine Learning models with Visualization using Python (MatPlotlib, Scikitlearn)

Course outcome (Course Skill Set)

At the end of the course the student will be able to :

Sl. No.	Description	Blooms Level
CO1	Familiarize with the issues and technologies involved in designing a wireless and mobile system that is robust against various attacks.	L1
CO2	Gain knowledge and understanding of the various ways in which wireless networks can be attacked and trade-offs in protecting networks.	L2
CO3	Have a broad knowledge of the state-of-the-art and open problems in wireless and mobile security, thus enhancing their potential to do research or pursue a career in this rapidly developing area.	L2
CO4	Learn various security issues involved in cloud computing.	L3
CO5	Learn various security issues related to GPRS and 3G.	L3

Mapping of COS and Pos

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	1							
CO2		2						2
CO3			3					
CO4					3			
CO5			2			3		