First Year Curriculum

Admission Year 2026-27

Master of Technology
CSE in Cyber Security

Faculty of Engineering & Technology

Parul University

Vadodara, Gujarat, India

Subject Syllabus
Advance Web Application Architecture and Security

Course: MTech- Cyber Security **Semester: 1**

Prerequisite: Basic knowledge of operating systems, networking, Linux fundamentals

Rationale: The security of digital infrastructure is an utmost need for an organization. The variety of security attacks makes it compulsion to analyze the way newer attacks are formed and their understanding is important to prevent or detect such attacks. The course aims to equip students with in-depth knowledge of web vulnerabilities, secure coding practices, and modern defense mechanisms. It focuses on identifying, analyzing, and mitigating security threats like SQL injection, XSS, CSRF, and authentication flaws. The course also emphasizes hands-on experience with security testing tools, penetration testing, and real-world attack prevention strategies.

Teaching and Examination Scheme

Teaching Scheme					Examination Scheme					Total
					Internal Marks			External Marks		
Lecture Hrs/Week	Tutorial Hrs/Week	Lab Hrs/Week	Hrs/Week	Credit	T	CE	P	T	P	
3	-	2	-	4	20	20	20	60	30	150

SEE- Semester End Examination, CIA- Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.)

Course Content

W - Weightage (%) ,**T** - Teaching hours

Sr.	Topics	W	T
1	**An Introduction to Web Application:** Understand web applications, how web application works, Client-Server Model, DNS, Web Application Proxy, Same Origin policies, Core Origin policies, Cookies, Sessions, Token, Browser Extensions, Google Hacking Database, C-panel introduction, Web Application vs Cloud Application, Future of Web Application.	15	7
2	**Web Application Security:** How does web security work, Web Application Lifecycle Maintenance, Importance of Web Application Security, Web Application Security vs Network Security, HTTP Request- Response, Web Application status codes. **Tools & Installation:** XAMPP, Burp-Suite, Burp-Suite Configuration with browser, Zap-Proxy, Nuclei, Use of GitHub, Footprinting tools, Enumeration tools, Wayback Machine, WP-Scan, Wappalyzer, Whatweb.net, NS-Lookup	25	11

3	**Web Application Vulnerabilities Assessment:** Vulnerability Assessment Concepts, Classification, and assessment types, Footprinting concepts, Footprinting through a search engine, Footprinting through Social Networking Sites, DNS footprinting, Host Discovery, Enumeration Concepts, Web site crawling, Finding Vulnerable parameters.	20	9
4	**Web Application Attacks-1:** Understanding OWASP, Understanding OWASP Top 10 Vulnerabilities, SQL Injections, SQL Map, Cross Site Scripting, Types of Cross Site Scripting, Advanced Phishing attacks, BeEF Framework, Defacements, Broken Access Control, Broken Authentication Session Management, Local File Inclusion, Remote file inclusion, Session hijacking, Clickjacking.	20	9
5	**Web Application Attacks-2:** OTP Bypass, Two Factor Authentication bypass, Cross-origin resource sharing, Business Logic Flaws, Business Logic Flaws, Cross-Site Request Forgery, CAPTCHA bypass, Insecure direct object reference, Mitigation Steps.	20	9

Reference Books	
1.	The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws – Dafydd Stuttard, Marcus Pinto
2.	Hacking Web Apps: Detecting and Preventing Web Application Security Flaws – Mike Shema
3.	Web Security for Developers: Real Threats, Practical Defense – Malcolm McDonald
4.	OWASP Testing Guide – OWASP Foundation

Course Outcome
After Learning the Course the students shall be able to:
1. Explain web application architecture by describing the client-server model, DNS, cookies, sessions, tokens, and web security policies. 2. Analyze web application security measures by comparing network security vs. web security, HTTP request-response mechanisms, and security lifecycle maintenance. 3. Utilize security tools by configuring XAMPP, Burp Suite, Zap-Proxy, and footprinting tools like WP-Scan, Wappalyzer, and NS-Lookup. 4. Assess web vulnerabilities by performing footprinting, enumeration, website crawling, and vulnerability assessments using various techniques. 5. Demonstrate web attack techniques and mitigation by exploring OWASP Top 10 vulnerabilities, SQL injection, phishing attacks, session hijacking, CAPTCHA bypass, and business logic flaws.

List of Practical	
1	To understand the architecture of web applications, client-server interactions, DNS resolution, and the role of web proxies.
2	To analyze HTTP requests and responses, understand status codes, and explore security mechanisms in web applications.
3	To install and configure security tools like XAMPP, Burp Suite, ZAP Proxy, Nuclei, and enumeration tools for web security assessments.
4	To perform reconnaissance using search engines, DNS footprinting, host discovery, and web crawling to identify vulnerabilities.
5	To exploit SQL injection vulnerabilities using SQLMap and manually extract sensitive database information.
6	To understand different types of XSS attacks, use BeEF framework, and conduct phishing simulations.
7	To use WPScan, Wappalyzer, WhatWeb, and Wayback Machine to identify web application vulnerabilities.
8	To perform Local File Inclusion (LFI), Remote File Inclusion (RFI), session hijacking, and Clickjacking attacks.
9	To bypass OTP, two-factor authentication, and CAPTCHA security mechanisms using various attack techniques.
10	To exploit CSRF vulnerabilities, understand business logic flaws, and demonstrate insecure direct object references (IDOR).

Subject Syllabus
Advance Mobile Application Architecture and Security

Course: MTech- Cyber Security **Semester: 1**

Prerequisite: Fundamentals of Android and iOS architecture Mobile rooting and Jailbreaking Understanding of IPA and APK

Rationale: With the rapid growth of mobile applications, security threats have become a major concern, leading to data breaches, unauthorized access, and privacy violations. This course equips students with the knowledge and hands-on skills to identify, assess, and mitigate security vulnerabilities in mobile applications. By understanding platform-specific security models, penetration testing techniques, and secure coding practices, students will be able to develop and test mobile apps that meet modern security standards.

Teaching and Examination Scheme

Teaching Scheme					Examination Scheme					Total
					Internal Marks			External Marks		
Lecture Hrs/Week	Tutorial Hrs/Week	Lab Hrs/Week	Hrs/Week	Credit	T	CE	P	T	P	
3	-	2	-	4	20	20	20	60	30	150

SEE- Semester End Examination, CIA- Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.)

Course Content

W - Weightage (%) ,**T** - Teaching hours

Sr.	Topics	W	T
1	**Introduction to Mobile Application Security** Overview of mobile app security landscape Risks and threats associated with mobile app development, Understanding security requirements for mobile apps, Mobile App Vulnerabilities, Common mobile app vulnerabilities and attack vectors Security issues related to platform-specific features (e.g. sensors, storage, etc.) Case studies and examples of mobile app vulnerabilities and exploits	25	10
2	**Introduction to IOS & IPA Applications:** History of iOS, Understanding iOS Hardware and Software Architecture, Understanding iOS Security Model, Understanding iOS Permission Model for Application Security, Sandboxing, Codesigning, Keychain and Encryption, Jailbreaking Devices, Understanding IPA Understanding Directories and Files on an IPA	15	8

3	**Secure Mobile App Static Analysis** Secure coding practices for mobile app development Mobile app threat modeling and risk assessment, Mobile app penetration testing and vulnerability assessments Designing secure mobile app architecture, Implementing secure authentication and access controls Securing mobile app communications	20	9
4	**Mobile Application Attacks 1:** Setting up Mobile App Pentesting Environment, Interact with the Devices, Starting with Drozer, Understanding AndroidManifest.xml, Configuring, Burp and Traffic Interception, Traffic Interception Bypass, Weak Server Side Controls, Insecure Data Storage, Insufficient Transport Layer Protection, Unintended Data Leakage, Poor Authentication & Authorization	20	9
5	**Mobile App Security Testing and Verification** Mobile app security testing techniques and methodologies Automating mobile app security testing Analyzing mobile app security testing results and identifying remediation steps	20	9

Reference Books

1.	The Mobile Application Hacker’s Handbook – Dominic Chell
2.	Android Hacker’s Handbook" – Joshua J. Drake
3.	iOS Hacker’s Handbook" – Charlie Miller
4.	Mobile Security and Privacy: Advances

Course Outcome
After Learning the Course the students shall be able to:
1. Identify mobile app security risks by analyzing threats, platform-specific vulnerabilities, and case studies of security exploits. 2. Evaluate common mobile vulnerabilities by examining attack vectors, insecure data storage, and platform-related security flaws. 3. Analyze iOS security architecture by exploring sandboxing, code signing, encryption, keychain security, and jailbreaking risks. 4. Perform secure mobile app development by implementing secure coding practices, authentication mechanisms, and secure data transmission. 5. Conduct mobile app security testing by setting up pentesting environments, using Drozer, analyzing traffic interception, and automating security assessments.

List of Practical	
1	To understand the mobile security landscape, threats, and security requirements for mobile application development.
2	To analyze common mobile app vulnerabilities, attack vectors, and platform-specific security risks.
3	To understand iOS architecture, security models, sandboxing, keychain encryption, and jailbreak techniques.
4	To analyze directories, files, and permission models in Android and iOS applications for security flaws.
5	To perform static code analysis, identify vulnerabilities in the source code, and apply secure coding practices.
6	To set up and configure a mobile app pentesting lab using Android Emulators, iOS Simulators, and security tools like Burp Suite and Drozer.
7	To intercept mobile app traffic using Burp Suite, analyze SSL/TLS security, and bypass certificate pinning.
8	To exploit security flaws such as weak server-side controls, insecure data storage, and authentication vulnerabilities.
9	To perform automated mobile app security testing using security tools and frameworks for vulnerability assessment.
10	To analyze security test results, identify remediation steps, and document findings in a professional security report.

Subject Syllabus
Advance Computer Network and Security

Course: MTech- Cyber Security **Semester: 1**

Prerequisite: Basics of Computer Network

Rationale: This course focuses on the design, analysis, and security of modern network architectures. It covers advanced networking concepts, threat modeling, intrusion detection, encryption techniques, and secures communication protocols. The course also emphasizes hands-on practice in securing networks, mitigating cyber threats, and implementing robust defense mechanisms.

Teaching and Examination Scheme

Teaching Scheme					Examination Scheme					Total
					Internal Marks			External Marks		
Lecture Hrs/Week	Tutorial Hrs/Week	Lab Hrs/Week	Hrs/Week	Credit	T	CE	P	T	P	
3	-	2	-	4	20	20	20	60	30	150

SEE- Semester End Examination, CIA- Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.)

Course Content

W - Weightage (%) ,**T** - Teaching hours

Sr.	Topics	W	T
1	**Introduction to Computer Network:** Types of networks, IP Address, NAT, IP Subnets, DHCP Server, Ports, DNS, Proxy Servers, Virtual Private Networks, DNS Server, OSI and TCP IP Model, Routers , Switches, Endpoint solutions, Access Directory, TOR Network.	15	8
2	**Types of Networks & policy:** Networking Devices (Layer1,2,3) - Different types of network layer attacks–Firewall (ACL, Packet Filtering, DMZ, Alerts and Audit Trails) – IDS,IPS and its types (Signature based, Anomaly based, Policy based, Honeypot based).	20	9
3	**VPNS:** VPN and its types –Tunneling Protocols – Tunnel and Transport Mode –Authentication, Header Encapsulation Security Payload (ESP)- IPSEC Protocol Suite, IKE PHASE 1, II, Generic Routing Encapsulation(GRE). Implementation of VPNs.	20	9

4	**Network Attacks :** Network Sniffing, Wireshark, packet analysis, display and capture filters, ettercap, DNS Poisoning, ARP Poisoning, Denial of services, Vulnerability scanning, Nessus, Network Policies, Open VAS, Sparta, Network Scanning Report Generation, System hardening, secure system configurations, SSL Striping, Setup network IDS/IPS, Router attacks, VPN Pentesting, VOIP, Pentesting,	25	10
5	**Wireless Attacks:** Protocols, MAC Filtering, Packet Encryption, Packet Sniffing, Types of authentication, ARP Replay attack, Fake Authentication Attack, De authentication, Attacks on WEP , WPA and WPA-2 Encryption, fake hotspots, evil twin attack, fluxion framework	20	9

Reference Books

1.	Computer Networking: A Top-Down Approach" – James F. Kurose, Keith W. Ross
2.	Network Security Essentials: Applications and Standards" – William Stallings
3.	Hacking Exposed: Network Security Secrets & Solutions" – Stuart McClure, Joel Scambray, George Kurtz
4.	Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems" – Chris Sanders

Course Outcome

After Learning the Course the students shall be able to:

1. Explain network fundamentals by detailing IP addressing, subnetting, DNS, VPNs, and the OSI/TCP-IP models along with their roles in communication.
2. Analyze network security policies by evaluating firewall configurations, IDS/IPS mechanisms, and network layer attack prevention techniques.
3. Implement secure VPN solutions by configuring tunneling protocols, authentication mechanisms, and IPSEC-based encryption methods.
4. Perform network attack simulations by using tools like Wireshark, Nessus, and OpenVAS to analyze vulnerabilities, sniff packets, and conduct penetration testing.
5. Assess wireless network security by exploring encryption methods, authentication protocols, and executing attacks like de-authentication and evil twin setups.

List of Practical

1	Configuring Network Components – Set up and configure IP addresses, NAT, DHCP, and analyze network communication using basic commands.
2	Subnetting and IP Addressing – Perform IP subnetting calculations and assign IPs to different network segments.
3	Setting Up and Configuring VPN – Implement a VPN using OpenVPN or IPsec and test secure data transmission.
4	Network Traffic Analysis Using Wireshark – Capture and analyze packets using Wireshark with display and capture filters.
5	Simulating ARP & DNS Poisoning Attacks – Perform ARP poisoning with Ettercap and DNS spoofing to manipulate network traffic.
6	Network Vulnerability Scanning – Scan a network for vulnerabilities using Nessus, OpenVAS, or Sparta and generate security reports.
7	Firewall and IDS/IPS Configuration – Configure firewall rules, set up an IDS/IPS (Snort/Suricata), and analyze intrusion alerts.
8	Wireless Network Attacks – Capture Wi-Fi traffic, perform deauthentication attacks, and crack WEP/WPA2 encryption using Aircrack-ng.
9	SSL Stripping and MITM Attacks – Demonstrate an SSL stripping attack using Bettercap and intercept HTTPS traffic.
10	VPN Penetration Testing – Perform security testing on VPN implementations to identify vulnerabilities and misconfigurations.

Subject Syllabus
Machine Learning

Course: M Tech **Semester: 1**

Prerequisite: Basic knowledge of programming in Python, Fundamental concepts of Mathematics, including Linear Algebra, Probability, and Statistics, Understanding of Data Structures and Algorithms for efficient data handling and processing.

Course Objective: The course aims to provide a comprehensive understanding of Machine Learning (ML) concepts, including supervised, unsupervised, and reinforcement learning, develop proficiency in decision tree learning, neural networks, and Bayesian learning, apply genetic algorithms, fuzzy logic, and optimization techniques to real-world problems, enable students to analyze and compare ML models based on accuracy, efficiency, and application, and implement ML models using Python/Java for text classification, face recognition, healthcare, and fraud detection.

Teaching and Examination Scheme

Teaching Scheme					Examination Scheme					Total
					Internal Marks			External Marks		
Lecture Hrs/Week	Tutorial Hrs/Week	Lab Hrs/Week	Hrs/Week	Credit	T	CE	P	T	P	
3	0	2	0	3	20	20	20	60	30	150

SEE- Semester End Examination, CIA- Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.)

Course Content

W-Weightage(%),**T**-Teaching hours

Sr.	Topics	W	T
1	**Introduction** Learning Problems, designing a learning system, Issues with machine learning. Concept Learning, Version Spaces and Candidate Eliminations, Inductive bias	10	5
2	**Supervised and Unsupervised learning** Decision Tree Representation, Appropriate problems for Decision tree learning, Algorithm, Hypothesis space search in Decision tree learning, inductive bias in Decision tree learning, Issues in Decision tree learning ,K- Nearest Neighbour Learning, Locally Weighted Regression, Radial Bases, Functions, Case Based Reasoning	24	12
3	**Artificial Neural networks and genetic algorithms** Neural Network Representation, Appropriate problems for Neural Network Learning, Perceptrons, Multilayer Networks and Back Propagation, Algorithms, Remarkson Back Propagation Algorithms, Case Study: face Recognition	18	7
4	**Bayesian Learning** Bayes Theorem, Bayes Theorem and Concept Learning, Maximum Likelihood and Least squared Error Hypothesis, Bayes Optimal Classifier, Gibbs Algorithm, Naïve Bayes	18	7

	Classifier,		
	Bayesian Belief Network, EM Algorithm Case Study: Learning to classify text.		
5	**Fuzzy Logic** Classical Logic and Fuzzy logic, Fuzzy Rule based systems, Fuzzy Decision making, Fuzzy Classification, Fuzzy Pattern Recognition, Applications	20	9
6	**Optimization Techniques** Derivative based Optimization –Descent Methods–Genetic Algorithms–Ant Colony Optimization–Particle Swarm Optimization, Case Study - fraud detection, health care using Soft computing techniques.	10	5

Reference Books

1	Real-World Machine Learning(Text Book) ByHenrik Brink, Joseph Richards, Mark Fetherolf | Dream Tech
2.	Pattern Recognition and Machine Learning By Bishop, Christopher | Springer
3.	Elements of Statistical Learning By Hastie, Tibshirani, and Friedman | Soft Computing for Problem Solving, AISC, Springer
4	Data Mining: Tools and Techniques By Jiawei Han and Michelline Kamber
5	Data Mining: A practical Machine Learning Tools and techniques By IH Witten, Eibe Frank, Mark A Hall | Elsevier

Course Outcome

After Learning the Course the students shall be able to:

Course Outcome: After learning the course the students will be able to:

1. Analyze various learning paradigms including concept learning, version spaces, and inductive bias in machine learning.
2. Implement and compare supervised and unsupervised learning algorithms, including Decision Trees, K-Nearest Neighbors, and Locally Weighted Regression for classification and regression tasks.
3. Design and train Artificial Neural Networks (ANNs) and apply genetic algorithms for solving real-world problems like face recognition.
4. Apply Bayesian Learning techniques, including Naïve Bayes Classifier, Bayesian Belief Networks, and the EM Algorithm, for tasks such as text classification.
5. Explore fuzzy logic and optimization techniques like Genetic Algorithms, Ant Colony Optimization,
   and Particle Swarm Optimization, and apply them in domains like fraud detection and healthcare.

Subject Syllabus
Machine Learning Laboratory

List of Practical

1	Dealing with Data using Numpy, Pandas, Statistics library
2	Data Analysis & Visualization on Diwali Sales Dataset.
3	Implement linear regression and logistic regression.
4	Implement the naïve Bayesian classifier for a sample training dataset stored as a .CSVfile, .Compute the accuracy of the classifier, considering a few test data sets.
5	Assuming a set of documents that need to be classified, use the naïve Bayesian Classifier model to perform this task.
6	Decision tree-based ID3 algorithm.
7	Write a program to implement the K-Nearest Neighbor algorithm to classify the iris data set
8	Apply EM algorithm to cluster a set of data stored in a .CSVfile, .Use the same data set for clustering using k-Means algorithm.
9	Write a program to construct a Bayesian network considering medical data. Use this model to demonstrate the diagnosis of heart patients using standard Heart Disease Data Set.
10	Compare the various supervised learning algorithm by using appropriate dataset.(Linear Regression, Support Vector Machine, Decision Tree)
11	Compare the various Unsupervised learning algorithm by using the appropriate datasets.(K Means Clustering, K Mode)
12	Build an Artificial Neural Network by implementing the Back propagation algorithm and test the same using appropriate data sets

Subject Syllabus
Applied Cryptography

Course: MTech- Cyber Security **Semester: 1**

Prerequisite: Introduction to Cryptography, familiarity with Elementary Number Theory, Linear Algebra, Probability & Statistics, Abstract Algebra, Discrete Mathematics, and Algorithms.

Rationale: This course equips students with essential cryptographic techniques to ensure data security and integrity. It covers encryption methods, cryptanalysis, number theory, public-key cryptography, and advanced topics like digital signatures and post-quantum cryptography. Students will gain the skills to design and implement secure cryptographic systems for modern security challenges

Teaching and Examination Scheme

Teaching Scheme					Examination Scheme					Total
					Internal Marks			External Marks		
Lecture Hrs/Week	Tutorial Hrs/Week	Lab Hrs/Week	Hrs/Week	Credit	T	CE	P	T	P	
3	-	2	-	4	20	20	20	60	30	150

SEE- Semester End Examination, CIA- Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.)

Course Content

W - Weightage (%) ,**T** - Teaching hours

Sr.	Topics	W	T
1	Data encryption standard, Double encryption, Triple encryption, Linear feedback shift register, Non-linear feedback shift register, Modern stream ciphers- Grain V1, Security in mobile telephony, Design specification of ZUC cipher (4G standard).	20	11
2	Pilling-up lemma, Discussion on CPA & CCA security, Cryptanalysis on block ciphers- linear and differential, Cryptanalysis on stream ciphers- correlation and algebraic.	20	7
3	Number Theory: Elliptic curve group, Square and multiply algorithm, Baby step giant step algorithm.	15	5
4	Public key encryption: Discussion about formulating security models, semantic security, indistinguishability, and decisional & search version of Diffie-Hellman assumption. RSA encryption and its security proof. Elgamal encryption and its security proof. Bilinear pairing. Digital Signature- security model, RSA digital signature and its security proof, elliptic curve digital signature algorithm (ECDSA). Identity-based encryption. Attribute-based encryption. Fully homomorphic encryption. Predicate encryption. Functional encryption.	25	11

5	Signal protocol. Commitment schemes. Zero-knowledge proofs. Introduction to post-quantum cryptography: Mathematical assumptions- SVP, CVP, SIS, LWE. Regev's encryption. GPV signature scheme and its security proof. Gentry-Sahai-Waters (GSW) fully homomorphic encryption scheme.	20	11

Reference Books

1.	Analyzing Computer Security -- Pfleeger and Pfleeger [Prentice Hall]
2.	Security in Computing – Pfleeger, Pfleeger, Shah {Pearson]
3.	Introduction to Computer Security -- Matt Bishop [Addison-Wesley]

Course Outcome

After Learning the Course the students shall be able to:

1. Implement encryption techniques like DES, Triple DES, and Grain V1.
2. Analyze cryptanalysis methods on block and stream ciphers.
3. Apply number theory using elliptic curves and cryptographic algorithms.
4. Develop secure encryption schemes with RSA, Elgamal, and homomorphic encryption.
5. Explore post-quantum cryptography with LWE, zero-knowledge proofs, and GPV signatures.

List of Practical	
1	Implementation of Data Encryption Standard (DES) – Encrypt and decrypt messages using DES, Double DES, and Triple DES.
2	Linear and Non-Linear Feedback Shift Registers – Implement LFSR and NLFSR for stream cipher generation.
3	Cryptanalysis of Block Ciphers – Perform linear and differential cryptanalysis on a given block cipher.
4	Cryptanalysis of Stream Ciphers – Analyze correlation and algebraic attacks on stream ciphers.
5	Elliptic Curve Operations – Implement elliptic curve group operations and the Square-and-Multiply algorithm.
6	Public Key Cryptography (RSA & ElGamal) – Implement RSA and ElGamal encryption and verify their security proofs.
7	Digital Signature Implementation – Generate and verify digital signatures using RSA and ECDSA.
8	Identity-Based and Attribute-Based Encryption – Implement a basic Identity-Based Encryption (IBE) and Attribute-Based Encryption (ABE) scheme.
9	Homomorphic Encryption – Implement basic Fully Homomorphic Encryption (FHE) operations using a given scheme.
10	Post-Quantum Cryptography Implementation – Implement lattice-based encryption using Learning With Errors (LWE) and analyze its security.

Subject Syllabus
Digital Forensic & Incident Response

Course: MTech- Cyber Security **Semester: 1**

Prerequisite: Basics of Computer Networks and Security, Operating Systems (Windows & Linux),
Programming Fundamentals (Python, Bash)

Rationale: With the increasing number of cyber threats, organizations require skilled professionals in Digital Forensics and Incident Response to analyze security breaches, collect evidence, and mitigate risks. This course equips students with practical skills to investigate cyber incidents, use forensic tools, and ensure compliance with legal frameworks.

Teaching and Examination Scheme

Teaching Scheme					Examination Scheme					Total
					Internal Marks			External Marks		
Lecture Hrs/Week	Tutorial Hrs/Week	Lab Hrs/Week	Hrs/Week	Credit	T	CE	P	T	P	
3	-	2	-	4	20	20	20	60	30	150

SEE- Semester End Examination, CIA- Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.)

Course Content

W - Weightage (%) ,**T** - Teaching hours

Sr.	Topics	W	T
1	**Introduction to Digital Forensics & Incident Response:** Overview of Cybercrime & Digital Forensics, Types of Digital Evidence & Chain of Custody, Digital Forensic Process (Identification, Collection, Preservation, Analysis, Reporting), Role of Incident Response in Cybersecurity, Forensic Tools Overview (Autopsy, FTK, EnCase, Volatility, Wireshark), Case Studies on Cybercrime Investigations	18	8
2	**Disk, File System & Memory Forensics:** Understanding File Systems (FAT, NTFS, EXT4), Disk Forensics: Data Acquisition & Recovery Techniques, File Metadata Analysis & Hidden Files, Memory Forensics: Volatility Framework, RAM Analysis, Process Dumping & Malware Detection, Windows Registry & Event Logs Analysis	22	10
3	**Network & Malware Forensics:** Network Forensics Fundamentals (Packets, Protocols, Traffic Analysis), Log Analysis (Firewall, IDS/IPS, SIEM Logs), Wireshark & TCPDump for Traffic Inspection, Malware Analysis (Static vs. Dynamic Analysis), Reverse Engineering Malware (IDA Pro, Ghidra), Ransomware, Keyloggers & Trojan Investigation	20	9

4	**Mobile & Cloud Forensics:** Mobile Forensics Challenges (Android & iOS), Data Acquisition from Mobile Devices (Logical vs. Physical), Mobile App Forensics & SQLite Database Analysis, Cloud Forensics (AWS, Azure, Google Cloud), Cloud Log Analysis & Evidence Collection, Challenges in Cloud Investigations (Legal & Technical)	20	9
5	**Legal, Ethical & Reporting Aspects of Digital Forensics:** Cyber Laws & Compliance (GDPR, HIPAA, PCI-DSS), Evidence Handling & Admissibility in Court, Ethics in Digital Forensics, Writing Forensic Reports & Presenting Evidence, Future Trends in DFIR (AI in Forensics, Automated Incident Response)	20	9

Reference Books

1.	"Incident Response & Computer Forensics" – Kevin Mandia, Chris Prosise
2.	"Digital Evidence and Computer Crime" – Eoghan Casey
3.	"Practical Malware Analysis" – Michael Sikorski, Andrew Honig
4.	"The Art of Memory Forensics" – Michael Hale Ligh

Course Outcome

After Learning the Course the students shall be able to:

1. Gain foundational knowledge of digital forensics and cyber incident response strategies.
2. Perform forensic investigations on various digital devices and extract evidence.
3. Analyze network logs, memory dumps, and malware artifacts.
4. Apply forensic methodologies for Windows, Linux, and mobile devices.
5. Demonstrate legal and ethical procedures in forensic investigations.

List of Practical	
1	To install and configure forensic tools and set up a virtual environment for conducting digital investigations.
2	To create a forensic disk image and recover deleted files using forensic tools.
3	To extract and analyze forensic artifacts from the Windows registry and system logs to detect user activity and system changes.
4	To analyze a RAM dump using the Volatility framework to detect running processes, malware infections, and security breaches.
5	To capture and analyze network traffic using Wireshark to identify suspicious connections and potential security threats.
6	To perform malware analysis using sandboxing techniques to understand its behavior, identify Indicators of Compromise (IoCs), and detect malicious code.
7	To analyze web browsing history, cookies, and email headers to detect phishing attempts and data exfiltration.
8	To acquire, extract, and analyze mobile device data, including call logs, messages, and application databases for forensic evidence.
9	To investigate security incidents in cloud environments by analyzing cloud service logs and detecting unauthorized access.
10	To simulate a ransomware attack, analyze the encrypted files, and develop an incident response and mitigation strategy.
11	To understand forensic documentation standards, write forensic investigation reports, and ensure compliance with legal and regulatory frameworks.
12	To apply forensic investigation skills in a real-world challenge by analyzing forensic images, extracting artifacts, and solving a digital crime scenario.

Subject Syllabus
System Hacking with MSF

Course: MTech- Cyber Security **Semester: 1**

Prerequisite: Understanding of Networking Concepts, Operating System Concepts, Kali Linux

Rationale: This course focuses on ethical hacking techniques using Metasploit Framework (MSF) and cryptographic security measures. It covers system exploitation, privilege escalation, payload delivery, encryption methods, and cryptographic attack mitigation. The course provides hands-on experience in penetration testing, secure communication, and cryptographic implementations to strengthen system security.

Teaching and Examination Scheme

Teaching Scheme					Examination Scheme					Total
					Internal Marks			External Marks		
Lecture Hrs/Week	Tutorial Hrs/Week	Lab Hrs/Week	Hrs/Week	Credit	T	CE	P	T	P	
3	-	2	-	4	20	20	20	60	30	150

SEE- Semester End Examination, CIA- Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.)

Course Content

W - Weightage (%) ,**T** - Teaching hours

Sr.	Topics	W	T
1	**Advanced Metasploit Architecture & Exploit Development** Deep Dive into Metasploit Architecture, Understanding Ruby-based Metasploit Modules, Exploit Development Fundamentals, Buffer Overflow & Return-Oriented Programming, Writing Custom Exploits, Fuzzing for Vulnerabilities using Metasploit, Shellcode Analysis & Development, Creating & Injecting Custom Shellcode, Understanding NOP Sleds and Payload Delivery.	15	8
2	**Advanced Reconnaissance & Vulnerability Exploitation** Custom Reconnaissance Techniques, Advanced Port Scanning & OS Fingerprinting, Deep Packet Inspection & Traffic Analysis, DNS Poisoning & Spoofing with Metasploit, Exploiting Enterprise Systems, Active Directory Exploitation (Kerberos & NTLM Attacks), SMB & RDP Exploitation Techniques, Database Attacks (SQL Injection, Exploiting PostgreSQL, MySQL, MSSQL), Cloud & Container Exploitation, AWS, Azure, and GCP Reconnaissance, Kubernetes & Docker Exploitation, Attacking Cloud APIs with Metasploit.	25	10

3	**Advanced Post-Exploitation & Persistence Techniques** In-Depth Meterpreter Usage, Process Injection & Migration, Keylogging & Screenshots with Metasploit, Fileless Malware Execution using Meterpreter, Privilege Escalation & Lateral Movement, Kernel Exploits for Escalation (Dirty COW, PrintNightmare, etc.), Token Impersonation & Pass-the-Hash Attacks, Exploiting Windows & Linux for Lateral Movement, Custom Backdoors & Persistence, Creating Undetectable Backdoors (C2 Servers), Trojanized Executables & DLL Injection, Registry & Startup Persistence Techniques.	20	9
4	**Anti-Forensics, Evasion & Advanced Payloads** Bypassing Modern Security Mechanisms, Evading AV, EDR, and SIEM Solutions, Polymorphic & Encrypted Payloads, Using Shikata Ga Nai, Veil Framework & Obfuscation Tools, Advanced Payload Development, Custom Msfvenom Payloads for Windows, Linux, and macOS, Multi-stage Payloads for Stealth Attacks, Exploiting ARM & IoT Devices using Custom Payloads, Web Exploitation & Social Engineering, Exploiting JavaScript & XSS with Metasploit, Automating Phishing Attacks using Metasploit & SET, Creating Malicious Documents (Macro & HTA Payloads).	20	9
5	**Real-World Attack Simulations & Defensive Strategies** Advanced Red Team Exercises, Simulated Attacks on Enterprise Networks, Full-Chain Exploitation (Initial Access → Persistence → Exfiltration), Bypassing Enterprise Defenses, Analyzing SIEM Logs for Attack Traces, Evading Security Controls (Splunk, ELK, Sysmon), Defensive & Incident Response Techniques, Detecting & Stopping Metasploit Attacks, Reverse Engineering Metasploit Payloads, Digital Forensics & Threat Hunting Against Metasploit, Capstone Project, Design & Execution of an Advanced APT (Advanced Persistent Threat) Attack Simulation, End-to-End Offensive Security Assessment.	20	9

Reference Books

1.	Mastering Metasploit – Nipun Jaswal
2.	The Art of Exploitation – Jon Erickson
3.	Black Hat Python: Python Programming for Hackers and Pentesters – Justin Seitz
4.	Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software – Michael Sikorski, Andrew Honig

Course Outcome

After Learning the Course the students shall be able to:

1. To perform Penetration Testing Using Metasploit.
2. To conduct Advanced Information Gathering and Exploitation.
3. To apply Cryptographic Techniques for Secure Communication.
4. To analyze the working of blockchain technology, Bitcoin transactions, wallets, mining, and their security implications.
5. To implement Classical and Modern Cryptographic Algorithms.

List of Practical

1	Installing and Setting Up Metasploit – Install Metasploit on Windows and Linux, configure the environment, and explore its framework.
2	Exploring Metasploit Console and Modules – Understand MSF console, run basic commands, and explore Metasploit components.
3	Information Gathering with Metasploit – Perform network enumeration, port scanning (Nmap), SMB scanning, and SNMP enumeration.
4	Password Sniffing and SSH Version Detection – Use Metasploit for password sniffing, detecting SSH versions, and brute-force attacks.
5	Client-Side Exploitation with Meterpreter – Exploit Windows machines, execute meterpreter commands, escalate privileges, and dump hashes.
6	Creating Payloads with msfvenom – Generate custom payloads using msfvenom, analyze exploit execution, and bypass basic security defenses.
7	Social Engineering and Browser Exploitation – Use social engineering techniques and test Browser Autopwn to exploit client-side vulnerabilities.
8	Message Authentication and Hashing – Implement MD5, SHA, and digital signatures, and analyze their security properties.
9	Understanding Bitcoin and Blockchain Transactions – Set up a Bitcoin wallet, analyze blockchain operations, and simulate a Bitcoin transaction.
10	Classical and Modern Cryptographic Ciphers – Implement Caesar, Vigenère, AES, and RSA encryption, and perform key exchange using Diffie-Hellman.

Subject Syllabus
Research Methodology & IPR

Course: MTech- Cyber Security **Semester: 1**

Prerequisite: Basic Research Knowledge

Rationale: To introduce students to the fundamental concepts of research methodology, including problem formulation, research design, and data analysis. To develop skills in writing research papers, technical reports, and thesis documentation with ethical considerations.

Teaching and Examination Scheme

Teaching Scheme					Examination Scheme					Total
					Internal Marks			External Marks		
Lecture Hrs/Week	Tutorial Hrs/Week	Lab Hrs/Week	Hrs/Week	Credit	T	CE	P	T	P	
4	0	0	-	4	20	20	-	60	-	100

SEE- Semester End Examination, CIA- Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.)

Course Content

W - Weightage (%) ,**T** - Teaching hours

Sr.	Topics	W	T
1	**Introduction:** **Research:-** Definition, Characteristics, Motivation and Objective, Research Methods vs Methodology, Types of Research – Descriptive vs Analytical, Applied vs Fundamental, Quantitative vs Qualitative, Conceptual vs Empirical.	10	5
2	**Methodology:** Research Process, Formulating the Research Problem, Defining the Research Problem, Research Questions, Research Methods vs. Research Methodology.	10	5
3	**Literature Review:** Review Concepts and Theories, Identifying and Analyzing the Limitations of Different Approaches.	15	6
4	**Formulation and Design:** Concept and Importance in Research, Features of a Good Research Design, Exploratory Research Design, Concept, Types and Uses, Descriptive Research Designs, Concept, Types and Uses, Experimental Design: Concept of Independent & Dependent Variables.	15	6

5	**Data modeling and Simulations:** Mathematical modeling, experimental skills, simulation skills, data analysis and interpretation.	10	5
6	**Technical writing and Technical presentations** Introduction to Technical Writing, Types of Technical Documents, Structure of Technical Documents, Writing Process and Style.	10	5
7	**Creativity and ethics in research, Intellectual property rights:** Definition and importance of creativity in scientific research, Techniques for Enhancing Creativity, Importance of ethics in scientific research, Plagiarism and data fabrication, Definition and importance of Intellectual Property Rights, Role of IPR in research, innovation, and commercialization, Types of Intellectual Property, Patents: Criteria for patentability, patent life cycle, patent infringement, Copyrights: Rights of authors, fair use policy, software copyrights	20	8
8	**Tools and techniques for research** Methods to Search Required Information Effectively, Reference Management Software, Software for Paper Formatting, Software for Detection of Plagiarism	10	5

Reference Books

1.	Kothari, C.R. – **Research Methodology: Methods and Techniques**
2.	Ranjit Kumar – **Research Methodology: A Step-by-Step Guide for Beginners**
3.	Wayne Goddard and Stuart Melville – **Research Methodology: An Introduction**
4.	Prabuddha Ganguli **- Intellectual Property Rights**

Course Outcome
After Learning the Course the students shall be able to:
1. To develop a fundamental understanding of research terminology, methodologies, and various approaches to conducting research. 2. To apply the concept in writing the technical content. 3. To evaluate the proposed work and compare with existing approaches systematically using the appropriate methodology, through simulation depending upon the research field. 4. To design algorithms using concepts learned and write reports and papers technically and grammatically correct. 5. Demonstrate knowledge of Intellectual Property Rights (IPR) and apply the process of patent drafting, filing, and searching at national and international levels.

Subject Syllabus
Security Monitoring

Course: MTech- Cyber Security **Semester: 2**

Prerequisite: Fundamentals of network security, working sensors, IPS/IDS, Snort, Suricata, and firewall log analysis for threat detection and prevention.

Rationale: The rising cyber threats, effective security monitoring and incident response are essential for threat detection and mitigation. This course equips students with skills in log management, SIEM, and SOC operations to enhance cyber security frameworks and respond to incidents proactively.

Teaching and Examination Scheme

Teaching Scheme					Examination Scheme					Total
					Internal Marks			External Marks		
Lecture Hrs/Week	Tutorial Hrs/Week	Lab Hrs/Week	Hrs/Week	Credit	T	CE	P	T	P	
3	-	2	-	4	20	20	20	60	30	150

SEE- Semester End Examination, CIA- Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.)

Course Content

W - Weightage (%) ,**T** - Teaching hours

Sr.	Topics	W	T
1	**Introduction to Security Operations & Threat Landscape** Introduction to SOC, Role and Responsibilities of SOC, SOC Maturity Models (SOC 1, 2, 3), SOC vs. NOC (Network Operations Center), Cyber Threat Landscape, Cyber Kill Chain & MITRE ATT&CK Framework, Common Cyber Threats (Phishing, Malware, Ransomware, APTs, etc.), Threat Intelligence & its Role in SOC, Security Incident Lifecycle, Identification, Containment, Eradication, Recovery, Incident Response Methodologies, SOC Team Structure (Tiers 1, 2, 3).	10	5
2	**SIEM & Log Management in SOC:** Security Information and Event Management (SIEM), Introduction to SIEM Solutions (Splunk, ELK Stack, IBM QRadar, ArcSight), Log Collection, Correlation, and Analysis, Rule-Based and Behavioral Analysis, Log Sources & Analysis, Windows Event Logs, Linux Syslogs, Firewall, IDS/IPS, Proxy Logs, Web Server, Cloud, and Application Logs, Threat Hunting Using SIEM, Proactive Threat Hunting Techniques, Anomaly Detection & Use Case Development, MITRE ATT&CK Mapping in SIEM.	20	8

3	**Security Monitoring & Threat Detection** Network Security Monitoring (NSM), Network Packet Analysis (Wireshark, Zeek, Suricata), IDS/IPS Solutions (Snort, Suricata), Malware Traffic Analysis, Endpoint Security Monitoring, EDR/XDR Solutions (CrowdStrike, Microsoft Defender, SentinelOne), Host-based Threat Detection, Behavioral & Signature-Based Detection, Threat Intelligence Integration, Open Source Intelligence (OSINT), Threat Intelligence Platforms (MISP, Anomali, Recorded Future), Integrating Threat Feeds into SOC.	20	8
4	**Incident Response, Digital Forensics & Attack Simulations** Incident Response (IR) Process, IR Frameworks (NIST, SANS), Incident Handling & Containment Strategies, Reporting & Documentation of Security Incidents, Digital Forensics & Investigation, Memory & Disk Forensics (Volatility, Autopsy), Network Forensics & Log Analysis, Malware Reverse Engineering Basics, Red Team vs. Blue Team Exercises, Simulating Attacks with Adversary Emulation (Atomic Red Team, Caldera), Purple Teaming Concepts, SOC Metrics & KPIs for Performance Evaluation.	25	12
5	**Compliance, Risk Management & SOC Automation** Security Compliance & Regulations, ISO 27001, NIST, GDPR, PCI-DSS, HIPAA, Compliance Monitoring & Audit Preparation, Risk Management & Vulnerability Management, Risk Assessment Frameworks (NIST RMF, FAIR), Vulnerability Scanning & Patch Management (Nessus, OpenVAS), SOC Automation & Orchestration, Security Orchestration, Automation, and Response (SOAR), Automating Incident Response with Playbooks, AI & Machine Learning in SOC.	25	12

Reference Books

1.	The Practice of Network Security Monitoring – Richard Bejtlich
2.	Applied Network Security Monitoring – Chris Sanders & Jason Smith
3.	Security Monitoring – Chris Fry & Martin Nystrom
4.	Network Security Monitoring – Niels Provos & Thorsten Holz
5.	Cybersecurity Blue Team Toolkit – Nadean Tanner

Subject Syllabus
Security Monitoring

Course Outcome

After Learning the Course the students shall be able to:

1. Establish SOC operations by defining roles, responsibilities, and security incident lifecycle.
2. Implement SIEM solutions for log management, correlation, and threat hunting.
3. Deploy security monitoring tools like IDS/IPS, EDR/XDR, and OSINT for threat detection.
4. Conduct incident response and digital forensics using industry-standard frameworks and tools.
5. Ensure compliance and automate SOC workflows using SOAR, AI, and regulatory frameworks.

List of Practical

1	**Security Operations & SOC Infrastructure Setup** Set up a basic Security Operations Center (SOC) environment using open-source tools like ELK Stack (Elasticsearch, Logstash, Kibana) or Security Onion. Analyze security flaws and define security goals in a given IT infrastructure
2	**Log Management Configuration** Configure log management on a Linux and Windows system. Set up centralized log collection using Syslog, Rsyslog, or Windows Event Forwarding (WEF).
3	**SIEM Tool Installation & Log Aggregation** Install a SIEM (Security Information and Event Management) tool such as Splunk, Wazuh, or Graylog. Collect and normalize logs from different sources (firewalls, endpoints, servers).
4	**Log Baselining & Correlation Rules** Establish a baseline of normal system logs. Create correlation rules to detect anomalies such as multiple failed login attempts.
5	**Incident Detection & Response Handling** Simulate a brute-force attack and monitor logs for detection. Respond to a failed login attempt scenario using predefined incident handling steps.
6	**Forensic Analysis & Evidence Collection** Capture and analyze logs from a compromised machine. Use Wireshark or Volatility for forensic analysis of system activity
7	**Incident Classification & Response Strategy** Categorize different types of security incidents based on severity. Formulate an incident response strategy for malware, insider threats, and phishing.
8	**SIEM-Based Threat Hunting** Use Splunk queries (SPL) or ELK searches to detect suspicious network activities. Investigate a simulated data exfiltration attempt using SIEM dashboards.

9	**Creating and Reviewing Security Reports** Generate a SOC report using SIEM or log management tools. Analyze false positives and false negatives in security alerts.
10	**Continuous Monitoring & Maintenance of SOC** Set up automated alerting for high-priority security incidents. Maintain cybersecurity monitoring policies and update them based on new threats.

Subject Syllabus
Cloud Computing & Security

Course: MTech- Cyber Security **Semester: 2**

Prerequisite: Understanding network terminologies, configurations, protocols, wireless networks, and cloud fundamentals, including network setup, communication standards, security considerations, and cloud-based networking principles for effective connectivity and management.

Rationale: Cloud computing is the backbone of modern IT infrastructure, but it comes with security challenges. This course equips students with cloud technologies, containerization, server less computing, cloud threats, and security best practices to build and secure cloud environments effectively.

Teaching and Examination Scheme

Teaching Scheme					Examination Scheme					Total
Lecture Hrs/Week	Tutorial Hrs/Week	Lab Hrs/Week	Hrs/Week	Credit	Internal Marks			External Marks		
					T	CE	P	T	P	
3	-	2	-	4	20	20	20	60	30	150

SEE- Semester End Examination, CIA- Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.)

Course Content

W - Weightage (%) ,**T** - Teaching hours

Sr.	Topics	W	T
1	**Introduction to Cloud Computing:** Cloud computing Concepts, Characteristics of cloud computing, Limitations of cloud computing, Types of cloud computing storage, Responsibilities model in cloud, Cloud deployment Models, NIST cloud deployment model, Cloud storage Architecture, AI in Cloud Computing, Cloud Service Providers.	15	6
2	**Cloud Computing Technology:** Introduction to Cloud technology, Container, Container Features, Container Architecture, Container lifecycle, Container Orchestration, Container vs Virtual machines, Docker, Docker engine, Docker Swarm, Docker Architecture, Docker Objects, Docker Operations, Microservices vs Docker, Docker Networking, Kubernetes, Kubernetes Features, Kubernetes Architecture, Kubernetes vs Docker, Container Security Challenges.	20	9

3	**Serverless Computing:** Serverless Computing, Advantages, disadvantages, Serverless vs Containers, Serverless Computing Framework. **Cloud Computing Threats:** Introduction OWASP, Introduction OWASP top 10 Risks, Serverless Security risks, Understanding risks- Loss of governance, Loss of encryption, Hardware failure, Supply Chain Failure, Isolation failure, VM-level Attacks	25	12
4	**Cloud Hacking:** Container Vulnerabilities, Kubernetes Vulnerabilities, Cloud Attacks: server hijacking using Social Engineering, Server hijacking using Network Sniffing, Side-Channel Attacks or Cross- guest VM, Wrapping Attack, Man-in-the-Cloud Attack, and many more attacks	20	9
5	**Cloud Security:** Cloud Security Control Layers, Cloud Security responsibility, Security Considerations, Placement of Security Controls in the cloud, Best Practices for Securing the cloud, NIST Recommendations for cloud Security, Kubernetes Vulnerabilities Solutions, Serverless Risk Solutions, Container Security, Docker Security, Zero trust Network.	20	9

Reference Books

1.	Cloud Security and Privacy – Tim Mather, Subra Kumaraswamy, Shahed Latif
2.	Kubernetes Up & Running – Kelsey Hightower, Brendan Burns, Joe Beda
3.	Docker Deep Dive – Nigel Poulton
4.	Cloud Computing: Principles and Paradigms – Rajkumar Buyya

Course Outcome
After Learning the Course the students shall be able to:
1. Explain cloud computing concepts including deployment models, storage architecture, and AI integration in the cloud. 2. Analyze cloud technologies such as containers, Kubernetes, Docker, and their security challenges. 3. Evaluate serverless computing by comparing it with containers and understanding its advantages and limitations. 4. Identify cloud computing threats including OWASP risks, VM-level attacks, and supply chain vulnerabilities. 5. Implement cloud security measures using best practices, NIST recommendations, and zero-trust security models.

List of Practical	
1	**Cloud Penetration Testing & Red Team Assessment** Perform a penetration test on a cloud-based application using tools like Metasploit, Nmap, and Burp Suite. Identify misconfigurations and exploit vulnerabilities in AWS, Azure, or GCP environments.
2	**Advanced Kubernetes Security - RBAC & Network Policies** Implement Role-Based Access Control (RBAC) in Kubernetes to restrict user privileges. Deploy network policies to restrict intra-cluster communication and prevent unauthorized access.
3	**Container Security Hardening & Runtime Protection** Use Docker Bench for Security to scan container misconfigurations. Implement Seccomp, AppArmor, and SELinux to restrict container behavior. Monitor runtime activity with Falco to detect security threats in real time.
4	**Cloud-Based Zero Trust Security Implementation** Implement a Zero Trust Architecture (ZTA) in a cloud environment. Use AWS Security Hub, Azure Defender, or Google Chronicle to enforce strict access control. Deploy BeyondCorp or Zscaler for identity-based cloud security.
5	**Exploiting & Mitigating Serverless Security Risks** Perform a serverless attack by exploiting vulnerable AWS Lambda or Azure Functions. Implement least privilege permissions and runtime monitoring to secure serverless functions.
6	**Cloud Threat Hunting & SIEM Log Analysis** Collect and analyze cloud logs using Splunk, ELK Stack, or Google Chronicle. Create custom SIEM correlation rules to detect brute-force attacks, insider threats, and privilege escalation.
7	**Implementing Cloud Forensics & Incident Response** Simulate a data breach in a cloud environment and collect forensic artifacts. Analyze AWS CloudTrail, Azure Security Center, or GCP Security Command Center logs to investigate security incidents.
8	**Cloud Cryptography & Data Protection** Encrypt sensitive S3 buckets or Azure Blob Storage with customer-managed keys (CMK). Implement Homomorphic Encryption or Attribute-Based Encryption (ABE) for secure cloud computing.
9	**Advanced Cloud Networking Security - VPC & API Gateway Protection** Configure Virtual Private Cloud (VPC) Peering and Service Mesh Security in Kubernetes. Secure API Gateways using OAuth 2.0, JWT, and API rate limiting to prevent DDoS attacks
10	**Cloud Attack Simulation with MITRE ATT&CK Framework** Simulate real-world cyberattacks on cloud environments using Atomic Red Team or Caldera. Map detected threats to MITRE ATT&CK Cloud Matrix and apply remediation strategies.

Subject Syllabus
Mobile and Wireless Communication Security

Course: MTech- Cyber Security **Semester: 2**

Prerequisite: Basic networking, cyber security fundamentals, wireless communication, OS concepts (Windows/Linux/Mobile), and security tools knowledge.

Rationale: With the rapid growth of wireless and mobile networks, ensuring security is critical to prevent cyber threats. This course equips students with the knowledge and skills to analyze vulnerabilities, implement security measures, and conduct risk assessments for WLANs and mobile devices. By understanding threats, exploits, and defense mechanisms, students will be prepared to secure modern wireless communication systems in real-world scenarios.

Teaching and Examination Scheme

Teaching Scheme					Examination Scheme					Total
					Internal Marks			External Marks		
Lecture Hrs/Week	Tutorial Hrs/Week	Lab Hrs/Week	Hrs/Week	Credit	T	CE	P	T	P	
3	-	2	-	4	20	20	20	60	30	150

SEE- Semester End Examination, CIA- Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.)

Course Content

W - Weightage (%) ,**T** - Teaching hours

Sr.	Topics	W	T
1	**Introduction to Wireless and Mobile Networks:** The evolution of data networks: Internet, computers, mobile phones, and network convergence. Basics of network security. Evolution of cybercrime. Wireless and mobile network security. Evolution from wired to wireless networking. OSI model. Economic and business impact of wireless networking. Introduction to the Internet of Things (IoT) and mobile IP security.	20	8
2	**Wireless LAN (WLAN) Security:** WLAN fundamentals: topologies, 802.11 standards, wireless access points, bridges, and antennas. WLAN and IP networking: threats, vulnerabilities, physical security, social engineering, wardriving. Wireless attacks: rogue APs, Bluetooth exploits, packet analysis, denial-of-service (DoS), peer-to-peer hacking. Basic WLAN security: authentication, access restriction, data protection, security implementation considerations.	20	10

3	**Advanced WLAN Security & Risk Assessment:** Comprehensive WLAN security policies: authentication, access control, data protection, and user segmentation. Managing network and user devices: security audits, ongoing management, and network risk assessments. WLAN auditing tools: discovery tools, penetration testing, password capture and decryption, hardware audits. WLAN risk assessment: IT security management, security audits, and risk mitigation strategies.	20	10
4	**Mobile Security Challenges and Models:** **Mobile security threats:** mobile phone vulnerabilities, exploit tools, Android, iOS, and Windows Phone security risks. Security models: Google Android, Apple iOS, Windows Phone security, BYOD security challenges. Mobile wireless attacks: scanning networks, client and infrastructure exploits, network and application-level threats. Mobile device security management: enterprise mobile security and defense mechanisms.	20	9
5	**Mobile Malware, Attacks, and Defense Strategies:** Mobile fingerprinting: identification techniques, software and device fingerprinting methods. Mobile malware: Android, iOS, and Windows malware threats, delivery methods, and defense strategies. Mobile device management (MDM): security policies, device monitoring, and penetration testing. Mobile network security: protecting mobile applications, phishing exploits, and incident response.	20	9

Reference Books

1.	Wireless and Mobile Device Security by Jim Doherty
2.	Mobile and Wireless Design Essentials by Martyn Mallick
3.	Mobile Communications by Jochen Schiller

Course Outcome
After Learning the Course the students shall be able to:
1. Explain wireless and mobile network security – evolution, OSI model, IoT, and mobile IP security. 2. Analyze WLAN security threats – authentication, rogue APs, DoS, and packet analysis. 3. Conduct WLAN security assessments – risk assessment, penetration testing, and security audits. 4. Evaluate mobile security models – Android, iOS, BYOD risks, and enterprise security. 5. Mitigate mobile malware threats – fingerprinting, malware analysis, and mobile network security.

Subject Syllabus
Mobile and Wireless Communication Security

List of Practical	
1	Wireless Network Scanning – Use tools like NetStumbler or Kismet to scan and analyze WLAN networks.
2	WLAN Packet Sniffing – Capture and analyze wireless traffic using Wireshark or Aircrack-ng.
3	WEP & WPA Cracking – Perform ethical Wi-Fi penetration testing using Aircrack-ng or Hashcat
4	Detecting Rogue Access Points – Identify unauthorized APs using Kismet and Wi-Fi Pineapple.
5	Bluetooth Security Testing – Analyze Bluetooth vulnerabilities using Bluesniff or BtleJuice.
6	Mobile Device Security Audit – Assess mobile security settings and vulnerabilities on Android & iOS.
7	Man-in-the-Middle (MITM) Attack Simulation – Use Ettercap or Bettercap to intercept wireless traffic (ethical use only).
8	Mobile Malware Analysis – Analyze Android malware behavior using MobSF or APKTool.
9	WLAN Penetration Testing – Perform penetration testing on Wi-Fi networks using Kali Linux tools.
10	Risk Assessment & Security Policy Implementation – Conduct a wireless network risk assessment and propose security policies.

Subject Syllabus
Blockchain Security

Course: MTech- Cyber Security **Semester: 2**

Prerequisite: Advanced computer networks, cryptography, blockchain development, cybersecurity, and blockchain technologies.

Rationale: Blockchain security is inherently interdisciplinary, relying on cryptography, distributed systems, and network security. A solid understanding of these foundational topics ensures students can effectively analyze and secure blockchain systems. The course focuses on identifying vulnerabilities, writing secure smart contracts, and defending against attacks, making prior knowledge of programming and cybersecurity essential for success in this area.

Teaching and Examination Scheme

Teaching Scheme					Examination Scheme					Total
					Internal Marks			External Marks		
Lecture Hrs/Week	Tutorial Hrs/Week	Lab Hrs/Week	Hrs/Week	Credit	T	CE	P	T	P	
3	-	2	-	4	20	20	20	60	30	150

SEE- Semester End Examination, CIA- Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.)

Course Content

W - Weightage (%) ,**T** - Teaching hours

Sr.	Topics	W	T
1	**Introduction to Blockchain Security:** History and evolution of blockchain technology, Key characteristics: Decentralization, immutability, consensus mechanisms, and cryptographic security, Overview of public vs. private blockchains, Role of trust in blockchain systems, Why blockchain security is critical for industries (e.g., finance, healthcare, supply chain). Confidentiality, integrity, and availability (CIA triad. Role of cryptographic techniques in securing blockchain data, Smart contracts and their security considerations, Blocks, chains, nodes, and distributed ledgers.	15	6
2	**Blockchain Technology:** Introduction to popular blockchain platforms: Ethereum, Hyperledger, Bitcoin, etc. ,Structure and design of blockchain, Peer-to-peer (P2P) network protocols, Smart Contracts and Decentralized Applications (DApps), Solidity programming language basics. Vulnerabilities in smart contracts (reentrancy, gas limit issues, etc.). Privacy in blockchain: Zero-knowledge proofs, ring signatures, and privacy-focused chains (e.g., Monero, Zcash), Security features and challenges of each platform.	20	9

3	**Blockchain Security Threats :** Overview of Security Threats in Blockchain , Attack surface and vectors: Nodes, smart contracts, consensus algorithms, and storage, General blockchain threats: 51% attack, Sybil attacks, Double-spending, and Transaction malleability, Smart Contract Vulnerabilities, Common vulnerabilities in smart contracts (e.g., integer overflow, gas usage problems, improper access control), Analyzing smart contract code for vulnerabilities, Eclipse attacks, man-in-the-middle attacks, and denial-of-service (DoS) attacks., Privacy leaks through improper encryption and lack of anonymization.	25	12
4	**Blockchain Hacking Techniques:** Understanding Blockchain Hacking, Introduction to ethical hacking and penetration testing for blockchain., Hacking cryptocurrencies: Wallets, exchanges, and private keys, Attack Methods on Blockchain, 51% Attacks: How attackers control the majority of mining power and their impact, Sybil Attacks: Creating fake nodes to overwhelm the network, Double-spending Attacks: Techniques for manipulating blockchain transaction history, Eclipse Attacks: Isolating nodes from the rest of the network, Smart Contract Exploits, Example case studies: DAO hack, Parity wallet vulnerability, Reverse-engineering smart contracts.	20	9
5	**Blockchain Security and Defense Mechanisms:** Securing Blockchain Networks, Node and network security practices (firewalls, intrusion detection systems, etc.), Cryptographic techniques for securing transactions (hashing, digital signatures, asymmetric encryption), Securing Smart Contracts, writing secure smart contracts, Auditing smart contracts: Tools and methodologies (MythX, Solhint, Slither), Preventing reentrancy and other common exploits, Consensus Algorithm Improvements, Evaluating the security of consensus mechanisms (PoW, PoS, etc.), Hybrid consensus mechanisms and their security, Overview of security frameworks for blockchain (e.g., ISO/IEC 27001, NIST Cybersecurity Framework), Developing security policies for blockchain implementations, Tools for Blockchain Security, Security tools for blockchain testing and analysis: Ganache, Truffle, Remix, and others, Penetration testing tools and practices for blockchain	20	9

Reference Books	
1.	"Blockchain Basics" by Daniel Drescher
2.	"Blockchain Applications: A Hands-On Approach" by Arshdeep Bahga and Vijay Madisetti
3.	"Mastering Bitcoin" by Andreas M. Antonopoulos
4.	"Blockchain Security" by Roger Wattenhofer

Course Outcome

After Learning the Course the students shall be able to:

1. Analyze blockchain security principles including decentralization, cryptographic security, and smart contract risks.
2. Evaluate blockchain platforms like Ethereum, Bitcoin, and Hyperledger, identifying security challenges and privacy solutions.
3. Identify blockchain security threats such as 51% attacks, Sybil attacks, and smart contract vulnerabilities.
4. Investigate blockchain hacking techniques including double-spending, eclipse attacks, and real-world exploit case studies.
5. Implement blockchain defense mechanisms using cryptographic security, secure smart contract development, and security frameworks.

List of Practical	
1	**Smart Contract Vulnerability Detection** Analyze a given Ethereum smart contract for common vulnerabilities such as reentrancy, integer overflow, and improper access control. Use tools like MythX, Slither, and Remix to identify security flaws and fix them.
2	**Penetration Testing on Blockchain Nodes** Conduct a penetration test on a blockchain node (e.g., Bitcoin or Ethereum) to identify common vulnerabilities such as DoS (Denial of Service), 51% attack potential, and network misconfigurations.
3	**Simulate a 51% Attack on a Private Blockchain** Set up a private blockchain network (using Hyperledger Fabric or Ethereum) and simulate a 51% attack to understand its impact on transaction integrity and consensus mechanisms
4	**Blockchain Transaction Forensics** Use blockchain analysis tools (e.g., Blockchair or Etherscan) to trace the flow of transactions and analyze how blockchain transaction data can be used for forensic investigations, focusing on privacy issues and transaction malleability.
5	**Implementing Zero-Knowledge Proofs (ZKPs)** Implement zero-knowledge proofs on a blockchain platform (e.g., Ethereum) to demonstrate how confidential transactions can be performed without revealing sensitive data, ensuring privacy while maintaining security.
6	**Secure Smart Contract Development** Write a secure smart contract for a decentralized application (DApp) using Solidity. Implement best practices for security such as ensuring proper gas limits, access controls, and checks for common vulnerabilities.
7	**Sybil Attack Simulation on a Test Blockchain Network** Set up a simulated test blockchain network and perform a Sybil attack by creating fake nodes. Evaluate the effect on consensus, block validation, and network reliability.
8	**Blockchain Privacy Protection Techniques** Use privacy-focused blockchains like Monero or Zcash and implement transaction obfuscation techniques (e.g., ring signatures and shielded transactions) to enhance privacy in blockchain applications.
9	**Blockchain Security Auditing with Truffle Suite** Perform a security audit of a smart contract using the Truffle Suite framework. Identify vulnerabilities in the contract's code and suggest improvements to secure it against attacks.
10	**Case Studies and Real-World Applications:** Real-world enterprise blockchain applications (supply chain, healthcare, banking). Addressing security issues in enterprise blockchain systems.

Subject Syllabus
Reverse Engineering and Malware Analysis

Course: MTech- Cyber Security **Semester: 2**

Prerequisite: Fundamentals of computer security and operating systems, programming (C, Python, Assembly), and networking protocols (TCP/IP, HTTP, DNS).

Rationale: Malware is a critical threat in cyber security, requiring specialized analysis techniques for detection and mitigation. This course equips students with static and dynamic malware analysis, reverse engineering, and behavior analysis skills to understand malicious software, detect threats, and develop effective countermeasures.

Teaching and Examination Scheme

Teaching Scheme					Examination Scheme					Total
Lecture Hrs/Week	Tutorial Hrs/Week	Lab Hrs/Week	Hrs/Week	Credit	Internal Marks			External Marks		
					T	CE	P	T	P	
3	-	2	-	4	20	20	20	60	30	150

SEE- Semester End Examination, CIA- Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.)

Course Content

W - Weightage (%) ,**T** - Teaching hours

Sr.	Topics	W	T
1	**Introduction to Reverse Engineering** Basic Concepts of Reverse Engineering, Disassembly Techniques, Assembly Language Fundamentals, and Decompilers and Their Limitations.	15	7
2	**Malware Analysis Fundamentals** Malware Types include Viruses, Worms, Trojans, Ransomware, and more. The Malware Lifecycle and Infection Vectors are key concepts in understanding how malware spreads. Static and Dynamic Malware Analysis Techniques are used to analyze malicious software, and Sandbox Environments play a crucial role in isolating malware for safe analysis.	20	9

3	**Binary Exploitation & Shellcode Analysis** Binary Exploitation includes Buffer Overflows, Integer Overflows, and Format String Vulnerabilities. Shellcode Analysis and Development are also key areas of focus.	20	9
4	**Advanced Malware Analysis & Anti-Reverse Engineering Techniques** Advanced Malware Analysis includes tools such as Disassemblers (IDA Pro), Debuggers (GDB, WinDbg), and Network Traffic Analysis Tools (Wireshark). It also covers Anti-Virus and Malware Detection Tools, along with Anti-Reverse Engineering Techniques, including Anti-Debugging Techniques, Anti-Disassembly Techniques, Packers and Unpacking, and Obfuscation Techniques.	25	11
5	**System-Level Analysis, Network Security & Legal Considerations** System-Level Analysis includes Windows System Internals, Linux System Internals, Registry Analysis, and File System Analysis. Network Security and Malware Analysis covers Network Protocols such as TCP/IP and HTTP, Network Traffic Analysis, Botnet Detection, and Advanced Persistent Threats (APTs). Legal and Ethical Considerations involve Digital Forensics Principles, Cybercrime Laws and Regulations, and Incident Response Methodologies.	20	9

Reference Books

1.	Practical Malware Analysis – Michael Sikorski & Andrew Honig
2.	The Art of Memory Forensics – Michael Hale Ligh, Andrew Case, Aaron Walters
3.	Reversing: Secrets of Reverse Engineering – Eldad Eilam
4.	Practical Reverse Engineering– Bruce Dang, Alexandre Gazet, Elias Bachaalany

Subject Syllabus
Reverse Engineering and Malware Analysis

Course Outcome

After Learning the Course the students shall be able to:

1. To perform Static and Dynamic Malware Analysis.
2. Gain knowledge of x86 assembly language and reverse engineering techniques.
3. To investigate Malware Behavior and Command & Control (C2) Mechanisms.
4. Analyze and Counter Self-Defending Malware Techniques.
5. Develop Effective Malware Mitigation Strategies.

List of Practical

1	Understand malware types, analysis techniques, and tools used in malware investigation.
2	Perform static analysis using hashing, antivirus scanning, and PE header inspection.
3	Execute malware in a sandboxed environment and monitor system behavior.
4	Analyze malicious code, Windows API calls, and registry modifications using IDA Pro.
5	Investigate malware persistence techniques, including registry modifications and scheduled tasks.
6	Study malware that evades detection using anti-debugging and anti-virtualization techniques.
7	Identify how malware maintains access through scheduled tasks, registry keys, and startup modifications.
8	Study how malware evades detection using anti-debugging, anti-virtualization, and packing techniques.
9	Analyze how malware interacts with C2 servers using HTTP, PowerShell, and custom protocols.
10	Learn to bypass obfuscation, unpack malware, and retrieve hidden payloads.

Subject Syllabus
Cyber Laws and Ethics

Course: MTech- Cyber Security **Semester: 2**

Prerequisite: Basic knowledge of operating systems, networking, Linux fundamentals

Rationale: The increasing number of cyber threats makes it essential to analyze emerging cybercrimes and understand their impact. This course provides an in-depth understanding of cybercrime, cyber law, and information security. It covers key legal frameworks, cybercrime issues, and the role of intermediaries, along with case studies to illustrate real-world applications. Additionally, it explores the intersection of intellectual property rights and cyber law, ensuring a comprehensive understanding of the digital legal ecosystem.

Teaching and Examination Scheme

Teaching Scheme					Examination Scheme					Total
					Internal Marks			External Marks		
Lecture Hrs/Week	Tutorial Hrs/Week	Lab Hrs/Week	Hrs/Week	Credit	T	CE	P	T	P	
3	-	2	-	4	20	20	20	60	30	150

SEE- Semester End Examination, CIA- Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.)

Course Content

W - Weightage (%) ,**T** - Teaching hours

Sr.	Topics	W	T
1	**Introduction to Cyber Crime and Cyber Law:** Introduction to cybercrime and cyber law, cyber space and information technology, Nature and scope of cybercrime, Jurisdiction of cybercrime.	15	8
2	**Cyber Crime Issues and Definitions under IT Act, 2000**: Important definitions under IT Act 2000, Cybercrime issues: unauthorized access, White collar crimes, viruses, malwares, worms, Trojans, logic bomb, Cyber stalking, voyeurism, obscenity in internet, Software piracy.	20	9
3	**Legal Framework for Cyber Crime:** IT Act, 2000 and Amendments: IT Act 2000, offences under IT Act and IT (amendment) Act, 2008. CRPC overview, Case studies, Role of intermediaries, Electronic evidence, Cyber terrorism, espionage, warfare and protected system.	20	9

4	**Amendments to Laws and Relevant Case Laws:** Overview of amended laws by the IT Act, 2000: The Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Banker's Book Evidence Act, 1891, The Reserve Bank of India Act, 1934, Cyber Theft and the Indian Telegraph Act, 1885. Relevant Case laws. Digital Signatures and certificate-legal issues.	20	9
5	**Intellectual Property Rights in the Digital Era:** Intellectual Property rights: Introduction to IP, Copyright, Related Rights, Trademarks, Geographical Indications, Industrial Design, Patents, Licensing and transfer of technology, WIPO Treaties, Copyrights Act, Patents Act, Trademarks Act.	25	10

Reference Books

1.	Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives by Raghu Santanam and M. Sethumadhavan, Information Science Reference.
2.	Security in Computing, 4th Edition by Charles P. Pfleeger and Shari L. Pfleeger, Upper Saddle River, NJ: Prentice Hall.
3.	Cybercrime: Security and Surveillance in the Information Age by Douglas Thomas and Brian Loader.
4.	Computer Crime: A Crime-Fighter's Handbook by David Icove.
5.	Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities by Peter N. Grabosky.
6.	Cyberlaw – The Indian Perspective by Pavan Duggal, Saakshar Law Publications.

Course Outcome

After Learning the Course the students shall be able to:

1. To describe the cyber world and cyber law in general and about the various facets of cyber crimes
2. Explore the Legal and Policy Developments in Various Countries to Regulate Cyberspace
3. Give Learners in Depth Knowledge of Information Technology Act and Legal Frame Work of Right to Privacy, Data Security and Data Protection.
4. To clarify the Intellectual Property issues in the cyber space and the growth and development of the law in this regard.

List of Practical

1	**Case Study 1: Jurisdiction in Cyber Crime** Case: A hacker from Russia defrauds an Indian e-commerce company by exploiting vulnerabilities in its payment gateway. The company wants to take legal action but faces jurisdictional challenges. Issue: How does cybercrime jurisdiction apply in cross-border cases? Discussion Points: Understanding the IT Act, 2000 jurisdiction clauses and international cooperation in cybercrime investigations.
2	**Case Study 2: Unauthorized Access and Hacking** Case: A disgruntled ex-employee of an IT firm gains unauthorized access to company servers and deletes critical files, causing major financial losses. Issue: Can the IT Act, 2000 hold the ex-employee liable for hacking? Discussion Points: Sections of the IT Act related to unauthorized access, penalties, and legal recourse
3	**Case Study 3: Cyber Stalking and Voyeurism** Case: A woman finds that a stranger is repeatedly harassing her online, sending obscene messages, and posting her edited photos on social media without consent. Issue: What legal protections exist under the IT Act, 2000 and IPC against cyber stalking and voyeurism? Discussion Points: Sections 354D IPC and IT Act provisions related to online harassment.
4	**Case Study 4: Malware and Ransomware Attacks** Case: A hospital's database is locked by ransomware, preventing doctors from accessing patient records. The attackers demand payment in cryptocurrency for decryption. Issue: How should organizations respond to ransomware attacks legally and technically? Discussion Points: Digital forensic investigation, reporting mechanisms, and cyber security measures.
5	**Case Study 5: Online Obscenity and Child Exploitation** Case: A social media platform is used to share obscene content involving minors. Authorities track the IP addresses of those involved and take legal action. Issue: How does the IT Act, 2000 address obscenity and child exploitation online? Discussion Points: Sections related to publishing/transmitting obscene material, role of intermediaries in content monitoring..
6	**Case Study 6: Software Piracy and Intellectual Property Rights Violation** Case: A software company finds that a pirated version of its product is being sold online at a fraction of the original price. Issue: How can the company protect its intellectual property under the Copyright Act and IT Act? Discussion Points: Legal actions available under the Copyright Act and IT Act, penalties for piracy.
7	**Case Study 7: Cyber Terrorism and Espionage** Case: A government agency detects an intrusion in its network from an unknown source, suspected to be a state-sponsored cyber espionage attack. Issue: How does the IT Act, 2000 define and handle cyber terrorism? Discussion Points: Legal provisions related to cyber terrorism, preventive measures, and penalties.

8	**Case Study 8: Banking Fraud and Phishing Attacks** Case: A victim receives an email pretending to be from their bank, asking them to update account details. After providing the information, their account is emptied. Issue: How can victims of phishing fraud seek legal recourse? Discussion Points: Cyber fraud prevention, banking security measures, and legal actions under the IT Act and RBI guidelines
9	**Case Study 9: Role of Intermediaries in Cyber Crime** Case: A messaging app is found to be used for spreading fake news and inciting violence. Authorities demand that the platform share user data, but the company refuses, citing privacy policies. Issue: What are the legal responsibilities of intermediaries under the IT Act? Discussion Points: Safe harbor provisions for intermediaries, content regulation, and privacy concerns.
10	**Case Study 10: Digital Evidence and Cyber Crime Investigation** Case: A person is accused of cyber fraud, but the main evidence is a series of emails. The accused claims the emails are fabricated. Issue: How is digital evidence verified and used in court? Discussion Points: Admissibility of electronic evidence under the Indian Evidence Act, forensic techniques for verifying emails and logs.

Subject Syllabus
Fundamentals of InfoSec, SCADA & IOT

Course: MTech- Cyber Security **Semester: 2**

Prerequisite: Basic knowledge of cyber security, network security, SCADA, IoT architecture, cryptography,
authentication, access control, cyber threats, and compliance standards.

Rationale: With increasing cyber security threats in SCADA and IoT systems, this course equips students to identify vulnerabilities, mitigate risks, and secure critical infrastructure.

Teaching and Examination Scheme

Teaching Scheme					Examination Scheme					Total
Lecture Hrs/Week	Tutorial Hrs/Week	Lab Hrs/Week	Hrs/Week	Credit	Internal Marks			External Marks		
					T	CE	P	T	P	
3	-	2	-	4	20	20	20	60	30	150

SEE- Semester End Examination, CIA- Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.)

Course Content

W - Weightage (%) ,**T** - Teaching hours

Sr.	Topics	W	T
1	**Fundamentals of Information Security:** Introduction to Information Security – CIA Triad (Confidentiality, Integrity, Availability), Threats, Vulnerabilities, and Risk Management, Cryptography & Secure Communication (Symmetric vs Asymmetric Encryption), Authentication, Authorization, and Access Control Mechanisms, Security Policies, Standards & Compliance (ISO 27001, NIST, GDPR, HIPAA), Secure Software Development Life Cycle (SDLC).	15	6
2	**Introduction to SCADA Security:** SCADA System Architecture & Components, SCADA Communication Protocols (Modbus, DNP3, IEC 60870-5-104), Cyber Threats & Attack Vectors in SCADA Systems, Case Studies on Real-World SCADA Cyber Attacks (Stuxnet, BlackEnergy), Security Hardening of SCADA Systems (Firewalls, Intrusion Detection), Role of AI/ML in SCADA Security	20	9

3	**Introduction to IoT & Its Security Challenges:** Overview of IoT – Architecture, Components, and Communication Protocols, IoT Device Security – Authentication, Firmware Security, Secure Boot, IoT Networking & Communication Security (MQTT, CoAP, Zigbee, 6LoWPAN), IoT Cloud Security & Data Privacy Concerns, IoT Risk Assessment & Security Testing Methodologies, Securing Smart Home, Smart Cities & Industrial IoT	20	12
4	**SCADA & IoT Cybersecurity Frameworks & Best Practices:** Industrial Cybersecurity Standards (IEC 62443, NIST 800-82), Threat Detection & Intrusion Prevention for SCADA & IoT, Incident Response & Digital Forensics in SCADA & IoT Environments, Security Audits & Vulnerability Assessments for Industrial Systems, Secure Remote Access & VPN Implementation for SCADA Systems, Case Studies – Best Practices in Industrial & IoT Security.	20	9
5	**Advanced Threats & Future Trends in SCADA & IoT Security:** Advanced Persistent Threats (APT) Targeting SCADA & IoT, AI-Powered Cyber Attacks & AI for Security Defense, Blockchain for IoT Security & Data Integrity, Quantum Computing and Its Impact on Cryptography, Secure Development and Deployment of SCADA & IoT Devices, Future Trends in Cybersecurity for Critical Infrastructure.	25	9

Reference Books

1.	"Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems" – Eric D. Knapp, Joel Langill
2.	"SCADA Security: What's Broken and How to Fix It" – Andrew Ginter
3.	"IoT Security: Practical Guide for Security Implementation in IoT Systems" – Dhananjay Gadre, Rajesh Singh
4.	"Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS" – Tyson Macaulay
5.	"The IoT Hacker's Handbook" – Aditya Gupta

Subject Syllabus
Fundamentals of InfoSec, SCADA & IOT

Course Outcome
After Learning the Course the students shall be able to:
1. Explain security basics – CIA Triad, risk, cryptography, and secure SDLC. 2. Analyze SCADA threats – attack vectors, case studies, and defenses. 3. Evaluate IoT security – authentication, networking, and cloud risks. 4. Apply cybersecurity frameworks – IEC 62443, NIST 800-82, and threat detection. 5. Explore future trends – AI attacks, blockchain security, quantum risks

List of Practical	
1	Introduction to Security Tools & Threat Simulation: Set up and configure security tools like Wireshark, Snort, and Metasploit for network analysis.
2	Vulnerability Assessment & Penetration Testing for SCADA Systems Perform security assessments using tools like Shodan, Nessus, and Nmap on SCADA devices.
3	IoT Device Enumeration & Security Testing Use IoT-specific testing tools (like IoT Inspector, Firmware Analysis Tools) to identify vulnerabilities.
4	Intrusion Detection & Prevention for Industrial Networks Configure IDS/IPS for SCADA/ICS environments and analyze alerts.
5	Secure Communication in SCADA & IoT Systems Implement encryption mechanisms like TLS/SSL, VPN, and SSH for secure data transmission.
6	Malware Analysis in SCADA & IoT Environments Analyze malware threats targeting industrial control systems and IoT devices.
7	Incident Response & Forensics for SCADA & IoT Cyber Attacks Perform forensic analysis using Volatility and Autopsy to investigate security breaches.
8	Firewall & Network Security Hardening for SCADA/IoT Configure firewalls and access controls to secure SCADA/IoT environments.
9	IoT Botnet Analysis & Mitigation Simulate an IoT botnet attack (like Mirai) and analyze mitigation techniques.
10	AI & Blockchain Implementation for IoT Security Use AI/ML for anomaly detection in IoT networks and implement blockchain-based security solutions.

Subject Syllabus
Advanced Database Security

Course: MTech- Cyber Security **Semester: 2**

Prerequisite: Basic knowledge of databases and SQL, Understanding of computer networks and Security concepts, Familiarity with operating systems and user access control.

Rationale: The growing volume of sensitive data stored in databases, ensuring database security is essential to prevent breaches, unauthorized access, and data loss. This course provides a comprehensive understanding of database security principles, models, and risk assessment techniques. Students will learn to configure security controls, manage vulnerabilities, implement access control models, and apply auditing mechanisms. By understanding threats such as SQL injection and perimeter security flaws, students will gain practical skills to secure database environments in real-world scenarios.

Teaching and Examination Scheme

Teaching Scheme					Examination Scheme					Total
					Internal Marks			External Marks		
Lecture Hrs/Week	Tutorial Hrs/Week	Lab Hrs/Week	Hrs/Week	Credit	T	CE	P	T	P	
3	-	2	-	4	20	20	20	60	30	150

SEE- Semester End Examination, CIA- Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.)

Course Content

W - Weightage (%) ,**T** - Teaching hours

Sr.	Topics	W	T
1	**Introduction to databases,** ACID properties, database security lifecycle, data classification, data risk assessment, database security architecture, feedback mechanisms.	15	7
2	**Data Preprocessing** Database installation and configuration: Profiles, passwords, privileges, and roles, databases security controls, security models, user administration.	20	9
3	**Database application security models:** Take-Grant Model, PN model, Bell and LaPadula Model, Biba Model, Clack-Wilson model, Lattice Model, Roll-based access control, XML databases.	20	9

4	**Database Vulnerabilities, Threats & Physical Security:** external and internal database threats, flaws in perimeter security, database security hierarchy, security in distributed databases, evaluate database security, evaluate organization's asset, system event triggers, flaws fixes and security patches, managing USB ports and USB enabled devices, database obscurity, virtual private database, SQL injection, backup mechanisms.	25	11
5	**Data security policy:** Database security risks, database security testing, database auditing models and tools, user management strategies, maintenance policy, assessment and (counter) measures.	20	9

Reference Books

1.	Database Security – A. Basta andM. Zgola [Cengage Learning]
2.	Database Security -- Castano, Fugini, Martella [Pearson]
3.	Database Security and Auditing-- Hassan Afyouni [Cengage Learning]
4.	Effective Oracle Database 10g Security by Design -- David C. Knox [McGraw-Hill]

Course Outcome

After Learning the Course the students shall be able to:

1. Explain database fundamentals, ACID properties, and the database security lifecycle.
2. Configure database security controls, user administration, and access management.
3. Analyze database security models, including Bell-LaPadula, Biba, and Role-Based Access Control.
4. Identify and mitigate database vulnerabilities, threats, and SQL injection attacks.
5. Implement database security policies, auditing mechanisms, and maintenance strategies.

List of Practical

1	**Database Installation & Configuration** Install a database management system (MySQL, PostgreSQL, or Oracle). Set up user profiles, passwords, privileges, and roles. Implement security controls (e.g., encryption, firewalls, and access control).
2	**Implementing ACID Properties** Create a sample database and demonstrate Atomicity, Consistency, Isolation, and Durability. Perform transactions and test rollback scenarios
3	**User Authentication & Role-Based Access Control (RBAC)** Create multiple users with different access roles. Implement role-based access control (RBAC). Restrict access to sensitive tables using SQL GRANT/REVOKE commands.
4	**Evaluating Database Security Architecture** Analyze database security risks using a risk assessment framework. Define a database security lifecycle for an organization.
5	**SQL Injection Testing & Prevention** Write vulnerable SQL queries and exploit them with SQL injection. Implement prepared statements or stored procedures to prevent SQL injection.
6	**Implementing Database Auditing & Logging** Enable database logging for tracking changes and access. Set up an auditing system to monitor unauthorized access.
7	**Configuring Virtual Private Databases (VPD)** Implement VPD in Oracle or PostgreSQL to restrict access to data based on user identity.
8	**Implementing Database Backup & Recovery** Create full, incremental, and differential backups. Test database restoration from backups.
9	**Identifying and Patching Database Vulnerabilities** Scan a database for security vulnerabilities using tools like SQLMap or Nessus. Apply security patches to fix detected vulnerabilities.
10	**Securing Physical & Network Access to Databases** Implement network-level security controls (e.g., firewalls, VPN, and SSL/TLS). Disable unnecessary USB ports to prevent unauthorized data extraction.

Subject Syllabus
Game Theory and Hacking

Course: MTech- Cyber Security **Semester: 2**

Prerequisite: Basic knowledge of cyber security, mathematical logic, networking, programming (Python, C, Java), and ethical hacking methodologies.

Rationale: This course explores game theory in cybersecurity, analyzing attacker-defender strategies and hacking techniques. It equips students with problem-solving skills to develop effective defense mechanisms. By integrating game theory with hacking, learners enhance security decision-making in real-world scenarios.

Teaching and Examination Scheme

Teaching Scheme					Examination Scheme					Total
Lecture Hrs/Week	Tutorial Hrs/Week	Lab Hrs/Week	Hrs/Week	Credit	Internal Marks			External Marks		
					T	CE	P	T	P	
3	-	2	-	4	20	20	20	60	30	150

SEE- Semester End Examination, CIA- Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.)

Course Content

W - Weightage (%) ,**T** - Teaching hours

Sr.	Topics	W	T
1	**Fundamentals of Game Theory in Cyber security:** Introduction to Game Theory and Cyber security Applications, Key Concepts: Nash Equilibrium, Zero-Sum Games, Non-Zero-Sum Games, Adversarial Thinking in Security & Attack-Defense Models, Strategic Decision Making in Cyber Warfare, Payoff Matrices, Mixed Strategies, and Utility Theory, Case Studies: Cyber War Games and Red-Blue Team Exercises.	15	6
2	**Attacker-Defender Games in Cybersecurity:** Modeling Cyber Attacks Using Game Theory, Stackelberg Security Games & Applications, Risk Assessment & Decision-Making in Cyber Attacks, Evolutionary Game Theory in Hacking Strategies, Deception & Honeypot Strategies Against Cyber Attacks, Practical Applications in Penetration Testing and Incident Response.	20	9

3	**Hacking Strategies & Game Theory Applications:** Understanding Adversarial Behavior & Risk Assessment, Cyber Deception & Defensive Strategy Games, Red Team vs Blue Team Methodology in Cybersecurity, Automated Attack-Defense Simulations & Cyber Range Scenarios, Reinforcement Learning and AI in Game-Theoretic Cybersecurity, Case Studies: Real-World Cyber Attacks and Strategic Countermeasures.	25	12
4	**Advanced Cybersecurity Threats & Countermeasures:** Zero-Day Exploits & Strategic Defense Approaches, Ransomware & Social Engineering: A Game-Theoretic Perspective, Multi-Agent Systems in Cybersecurity Decision-Making, Cryptographic Security Games: Secure Multi-Party Computation, AI and Adversarial Machine Learning in Cybersecurity, Mitigation Strategies Using Defensive Game Theory Models.	20	9
5	**Ethical Hacking & Cybersecurity Policies:** Legal & Ethical Implications of Hacking, Policy Making Using Game Theory in Cybersecurity, Cybersecurity Compliance and Risk Management, Digital Forensics & Cyber Threat Intelligence, Future of Cybersecurity in Game-Theoretic Frameworks, Case Study: Cybersecurity Strategies in National Defense.	20	9

Reference Books	
1.	"Game Theory for Security and Risk Management" – Stefan Rass, Stefan Schauer
2.	"Cybersecurity and Applied Mathematics" – Leigh Metcalf, William Casey
3.	"Introduction to Game Theory" – Martin J. Osborne
4.	"Hacking: The Art of Exploitation" – Jon Erickson
5.	"The Web Application Hacker's Handbook" – Dafydd Stuttard, Marcus Pinto
6.	"The Mathematics of Cybersecurity" – David J. Mussington

Parul® University

Subject Syllabus
Game Theory and Hacking

Course Outcome
After Learning the Course the students shall be able to:
1. Apply game theory to cybersecurity – Nash Equilibrium, attack-defense models, and strategic decision-making. 2. Model attacker-defender interactions – Stackelberg games, deception strategies, and penetration testing. 3. Analyze hacking strategies – AI-based defense, cyber deception, and adversarial simulations. 4. Examine advanced threats – zero-day exploits, ransomware, and cryptographic security games. 5. Integrate ethics and policy – legal frameworks, compliance, and cybersecurity in national defense.

List of Practical	
1	Simulating a Zero-Sum Game in Cybersecurity – Understanding Nash Equilibrium in attack-defense scenarios
2	Modeling an Attacker-Defender Strategy – Using Stackelberg security games for penetration testing.
3	Setting Up a Honeypot and Analyzing Attacker Behavior – Deception strategies for cyber defense.
4	Red Team vs. Blue Team Exercise – Simulating real-world attack and defense scenarios.
5	Conducting a Risk Assessment Using Game Theory – Identifying vulnerabilities in a network infrastructure.
6	AI-Based Adversarial Simulation – Implementing reinforcement learning in cybersecurity strategy.
7	Cryptographic Security Games – Analyzing key exchange and encryption using game-theoretic models.
8	Social Engineering Attack Simulation – Understanding phishing and deceptive attack strategies.
9	Analyzing Ransomware Strategies Using Game Theory – Evaluating attack mitigation methods.
10	Developing Cyber security Policies Using Game Theory – Strategic decision-making for security

Subject Syllabus
Deep Learning

Course: MTech- Cyber Security **Semester: 2**

Prerequisite: Linear Algebra and Probability, Fundaments of Machine learning

Rationale:: The objective of this course is to provide a comprehensive understanding of artificial neural networks (ANN) and deep learning models, including their architectures, training methodologies, and optimization techniques. It focuses on advanced neural network paradigms such as CNNs, RNNs, LSTMs,
and generative models for handling complex tasks in vision, speech, and natural language processing.

Teaching and Examination Scheme

Teaching Scheme					Examination Scheme					Total
					Internal Marks			External Marks		
Lecture Hrs/Week	Tutorial Hrs/Week	Lab Hrs/Week	Hrs/Week	Credit	T	CE	P	T	P	
3	-	2	-	4	20	20	20	60	30	150

SEE- Semester End Examination, CIA- Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.)

Course Content

W - Weightage (%) ,**T** - Teaching hours

Sr.	Topics	W	T
1	**Introduction to Neural Networks** Basics of Artificial Neural Networks (ANN): Artificial Neurons, Computational Models of Neurons, Structure of Neural Networks, and Functional Units of ANN for Pattern Recognition Tasks.	10	5
2	**Feed forward Neural Networks** Pattern Classification using Perceptron, Multilayer Feed forward Neural Networks (MLFFNNs), Back propagation Learning, Empirical Risk Minimization, Regularization, and Autoencoders.	10	5
3	**Feedforward Neural Networks** Pattern Classification using Perceptron, Multilayer Feedforward Neural Networks (MLFFNNs), Backpropagation Learning, Empirical Risk Minimization, Regularization, and Autoencoders.	15	7

4	**Convolution Neural Networks (CNNs)** Introduction to CNNs – Convolution, Pooling, Deep CNNs, Different Deep CNN Architectures – LeNet, AlexNet, VGG, PlacesNet. **Training a CNN:** Weights Initialization, Batch Normalization, Hyperparameter Optimization, and Understanding and Visualizing CNNs.	20	8
5	**Recurrent Neural Networks (RNNs)** Sequence Modeling using RNNs, Back propagation Through Time, Long Short-Term Memory (LSTM), Bidirectional LSTMs, Bidirectional RNNs, and Gated RNN Architecture.	20	8
6	**Generative Models** Restricted Boltzmann Machines (RBMs), Stacking RBMs, Belief Nets, Learning Sigmoid Belief Nets, Deep Belief Nets, Stochastic Autoencoders (AE), Variational Autoencoders (VAE), and Generative Adversarial Networks (GAN).	15	7
7	**Applications:** Applications in vision, speech, and natural language processing.	10	5

Reference Books

1.	Deep Learning (Textbook) by Ian Goodfellow, Yoshua Bengio, and Aaron Courville.
2.	Neural Networks and Deep Learning: A Textbook by Charu C. Aggarwal.
3.	Deep Learning with Python by François Chollet.

Subject Syllabus
Deep Learning

Course Outcome

After Learning the Course the students shall be able to:

1. Include artificial neurons, computational models, and their role in pattern recognition.
2. Identify and address challenges in training deep neural networks (DNNs) using advanced optimization techniques.
3. Design and train convolutional neural networks (CNNs) for image classification and feature extraction.
4. Implement recurrent neural networks (RNNs) and advanced architectures for sequence modeling and time-series applications.
5. Apply neural networks to real-world problems in vision, speech, and natural language processing (NLP) using deep learning.

Parul University

Subject Syllabus
Deep Learning

List of Practical	
1	**Implementation of Perceptron for Binary Classification:** Implement a single-layer perceptron for simple classification problems like AND, OR, and XOR gates. Train the perceptron using the delta rule and analyze convergence.
2	**Implementation of Multilayer Feedforward Neural Networks (MLFFNNs) with Backpropagation:** Design a three-layer feedforward neural network using backpropagation for digit classification (MNIST dataset).Apply empirical risk minimization and regularization techniques to avoid overfitting.
3	**Optimization Techniques for Deep Neural Networks:** Implement and compare optimization techniques such as SGD, AdaGrad, RMSProp, and Adam on a deep neural network. Evaluate the effect of different optimizers on training convergence and accuracy.
4	**Implementation of Convolutional Neural Networks (CNNs) for Image Classification:** Implement a CNN from scratch and train it on the CIFAR-10 or MNIST dataset. Experiment with convolution, pooling layers, and different activation functions.
5	**Transfer Learning using Pretrained Deep CNN Architectures:** Use pretrained models like AlexNet, VGG, or ResNet for image classification. Fine-tune the model on a custom dataset using hyperparameter optimization techniques.
6	**Understanding and Visualizing CNNs:** Implement Grad-CAM or feature map visualization to understand how CNNs make decisions. Analyze how different convolutional layers detect edges, textures, and high-level features.
7	**Implementation of Recurrent Neural Networks (RNNs) for Sequence Prediction:** Train an RNN model to predict a time-series dataset (e.g., stock price prediction).
8	**Long Short-Term Memory (LSTM) and Bidirectional LSTM for Text Generation:** Train an LSTM-based text generator using a dataset like Shakespeare's text or movie scripts. Experiment with bidirectional LSTMs and compare their performance with standard LSTMs.
9	**Implementation of Generative Adversarial Networks (GANs) for Image Generation:** Build a basic GAN and train it to generate handwritten digits (MNIST dataset). Experiment with loss functions, discriminator/generator balance, and regularization techniques.
10	**Implementation of Variational Autoencoders (VAEs) for Image Reconstruction:** Train a VAE for image reconstruction using the Fashion-MNIST dataset. Analyze the latent space representation and generate new images from the learned distribution.