JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
Minor in CYBER SECURITY
Course Structure & Syllabus (R-25 Regulations)
Applicable from AY 2025-2026 Batch

S.No	Year/ Semester	Theory (3 credits)	Lab (1 Credit)	Total Credits
1	II Year II Sem.	Principles of Information Security	Principles of Information Security Laboratory	4
2	III Year I Sem.	Foundations of Cyber Security	--	3
3	III Year II Sem.	Vulnerability Assessment and Penetration Testing **OR** Digital Forensics (Through MOOCS)	(The corresponding Laboratory) Vulnerability Assessment and Penetration Testing Laboratory **OR** Digital Forensics Laboratory	4
4	IV Year I Sem.	**Any one of the following subjects:** 1. Security Incident & Response Management 2.Mobile Security 3.IoT Security 4. Blockchain Technologies 5. Authentication Techniques 6. Cloud Security	--	3
5	IV Year I Sem.	Project/ Experiential Learning		4
			Total Credits	**18**

PRINCIPLES OF INFORMATION SECURITY

B.Tech. Cyber Security (Minor) II Year II Sem.

L	T	P	C
3	0	0	3

Prerequisites: A Course on “Mathematics”.

Course Objectives

1. To understand the fundamentals of Computer Networks.
2. To understand the fundamentals of Cryptography.
3. To understand various Symmetric and Asymmetric encryption algorithms.
4. To understand Mathematics of Cryptography, IDS and Firewalls.

Course Outcomes

- To apply algorithms used for message Integrity and Authentication.
- Demonstrate the knowledge of Computer Networks, Cryptography, Information security concepts and applications.
- Ability to apply security principles in system design.

UNIT - I

Introduction to Computer Networks, Network hardware, Network software, OSI and TCP/IP Reference models, Security attacks, Security Services and Mechanisms.

UNIT - II

Integer Arithmetic, Modular Arithmetic, Traditional Symmetric Key Ciphers, Data Encryption Standard (DES), Advanced Encryption Standard (AES).

UNIT - III

Mathematics of Cryptography: Primes, Primality Testing, Factorization, Chinese Remainder Theorem, Asymmetric Cryptography: Introduction, RSA Cryptosystem, Rabin Cryptosystem, Elliptic Curve Cryptosystem,

UNIT - IV

Message Integrity and Message Authentication: Message Authentication Code (MAC), SHA-512 , Digital Signatures.

UNIT - V

Security at the Application Layer: PGP and S/MIME. Security at Transport Layer: SSL and TLS. Principles of IDS and Firewalls.

TEXT BOOKS:

1. Computer Networks, Andrew S Tanenbaum, David. j. Wetherall, 5th Edition. Pearson Education/PHI.
2. Cryptography & Network Security by Behrouz A. Forouzan. Special Indian Edition, TMH.

REFERENCE BOOK:

1. Network Security Essentials (Applications and Standards), William Stallings Pearson Education.

PRINCIPLES OF INFORMATION SECURITY LAB

B.Tech. Cyber Security (Minor) II Year II Sem.

L	T	P	C
0	0	2	1

Pre-requisites: A Course on “Mathematics

Course Objectives

1. To apply algorithms on various Symmetric and Asymmetric encryption algorithms.
2. To demonstrate IDS Tools
3. To apply algorithms used for message Integrity and Authentication

Lab Exercises

1. Write a program to perform encryption and decryption using the following:
   a) Substitution cipher.
   b) Caeser cipher
   c) Play fair cipher
   d) Hill Cipher
2. Write a program to implement the DES algorithm.
3. Write a program to implement RSA algorithm.
4. Calculate the message digest of a text using the SHA-1 algorithm.
5. Working with sniffers for monitoring network communication (Wireshark).
6. Configuring S/MIME for email communication.
7. Using Snort, perform real time traffic analysis and packet logging.

TEXT BOOKS:

1. “Cryptography and Network Security” by William Stallings 3rd Edition, PearsonEducation.
2. “Applied Cryptography” by Bruce Schneier.

REFERENCE BOOK:

1. Cryptography and Network Security by Behrouz A. Forouzan.

FOUNDATIONS OF CYBER SECURITY

B.Tech. Cyber Security (Minor) III Year I Sem.

L	T	P	C
3	0	0	3

Prerequisites : Computer Programming.

COURSE OBJECTIVES:

To understand the difference between threat, risk, attack, and vulnerability.

To learn about security in operating system and networks.

To analyze the different security available in databases.

To understand the concept of privacy and security in emerging technologies.

To learn about management and risks in different technologies

COURSE OUTCOMES:

At the end of the course, the student should be able to:

1. Classify various types of attacks and learn the tools to launch the attacks.
2. Apply various tools to perform information gathering.
3. Analyze intrusion techniques to detect intrusion.
4. Apply intrusion prevention techniques to prevent intrusion.
5. Explain the basics of cyber security, cybercrime and cyber law.

UNIT I

INTRODUCTION TO CYBER SECURITY:

Introduction - Computer Security - Threats - Harm - Vulnerabilities - Controls -Authentication - Access Control and Cryptography – Web User Side - Browser Attacks -Web Attacks Targeting Users - Obtaining User or Website Data - Email Attacks.

UNIT II

SECURITY IN OPERATING SYSTEM AND NETWORKS

Security in Operating Systems - Security in the design of Operating Systems - Root Kit -Network Security Attack - Threats to Network Communications - Wireless Network Security- Denial of Service(DoS) - Distributed Denial-of-Service.

UNIT III

DEFENCES: SECURITY COUNTER MEASURES

Cryptography in Network Security - Firewalls - Intrusion Detection and Prevention Systems -Network Management - Databases - Security Requirements of Databases - Reliabilityand Integrity - Database disclosure - Data Mining and Big Data.

UNIT IV

PRIVACY IN CYBERSPACE

Privacy Concepts - Privacy Principles and Policies - Authentication and Privacy – Data Mining - Privacy on the Web - Email Security - Privacy impacts of Emerging Technologies.

UNIT V

MANAGEMENT AND INCIDENTS

Security planning - Business continuity planning - Handling incidents - Risk Analysis -Dealing with Disaster - Emerging Technologies - Internet of Things - Economics – Electronic Voting - Cyber Warfare- Cyberspace and the Law-International Laws-Cyber Crime-Cyber Welfare and Homeland security.

TEXT BOOKS:

1. Charles P. Pfleeger, Shari Lawrence Pfleeger and Jonathan Margulies, “Security in Computing”, 5th Edition, Pearson Education.
2. David Kim and Michael G. Solomon, “Foundations of Cyber Security”, Custom Edition, Jones and Bartlett Learning.

REFERENCES:

1. MarttiLehto, Pekka Neittaanmaki, “Cyber Security: Analytics, Technology and Automation”, Springer International Publishing Switzerland.
2. George K. Kostopoulous, “Cyber Space and Cyber Security”, CRC Press.

VULNERABILITY ASSESSMENT AND PENETRATION TESTING

B.Tech Cyber Security (Minor) III Year II Sem.

L	T	P	C
3	0	0	3

Prerequisites

1. Knowledge in information security.
2. Knowledge on Web Application.

Course Objectives"

- Give an introduction to Vulnerability Assessment and Penetration Testing.
- To be familiar with the Penetration Testing and Tools.
- To get an exposure to Metasploit exploitation tool, Linux exploit and Windows exploit.
- To gain knowledge on Web Application Security Vulnerabilities, Vulnerability analysis and Malware analysis.

Course Outcomes"

1. Learn to handle the vulnerabilities of a Web application
2. Able to learn various penetration testing tools.
3. Knowledge on Metasploit, Linux exploit and windows exploit tools
4. Analyze various vulnerabilities

UNIT-I

Introduction

Ethics of Ethical Hacking: Why you need to understand your enemy's tactics, recognizing the gray areas in security, Vulnerability Assessment and Penetration Testing.

Penetration Testing and Tools:

Social Engineering Attacks: How a social engineering attack works, conducting a social engineering attack, common attacks used in penetration testing, preparing yourself for face-to-face attacks, defending against social engineering attacks.

UNIT-II

Physical Penetration Attacks: Why a physical penetration is important? conducting a physical penetration, Common ways into a building, defending against physical penetrations.

Insider Attacks: Conducting an insider attack, defending against insider attacks.

Metasploit: The Big Picture, Getting Metasploit, Using the Metasploit Console to Launch Exploits, Exploiting Client-Side Vulnerabilities with Metasploit, Penetration Testing with Metasploit's Meterpreter, Automating and Scripting Metasploit, Going Further with Metasploit.

UNIT-III

Managing a Penetration Test: planning a penetration test, structuring a penetration test, execution of a penetration test, information sharing during a penetration test, reporting the results of a Penetration Test.

Basic Linux Exploits: Stack Operations, Buffer Overflows, Local Buffer Overflow Exploits, Exploit Development Process.

Windows Exploits: Compiling and Debugging Windows Programs, Writing Windows Exploits, Understanding Structured Exception Handling (SEH), Understanding Windows Memory Protections(XPSP3,Vista,7 and Server2008), Bypassing Windows Memory Protections.

UNIT-IV

Web Application Security Vulnerabilities:

Overview of top web application security vulnerabilities, Injection vulnerabilities, cross-Site scripting vulnerabilities, the rest of the OWASP Top Ten SQL Injection vulnerabilities, Cross-site scripting vulnerabilities.
Vulnerability Analysis:
Passive Analysis, Source Code Analysis, Binary Analysis.

UNIT-V
Client-Side Browser Exploits:
Why client-side vulnerabilities are interesting, Internet explorer security concepts, history of client-side exploits and latest trends, finding new browser-based vulnerabilities heap spray to exploit, protecting yourself from client-side exploit.
Malware Analysis: Collecting Malware and Initial Analysis: Malware, Latest Trends in Honeynet Technology, Catching Malware: Setting the Trap, Initial Analysis of Malware.

TEXT BOOKS:

1. Gray Hat Hacking-The Ethical Hackers Handbook", Allen Harper, Stephen Sims, Michael Baucom, 3rd Edition, Tata Mc Graw-Hill.
2. The Web Application Hacker's Handbook-Discovering and Exploiting Security flaws", Dafydd Suttard, Marcus pinto, 1st Edition, Wiley Publishing.

REFERENCE BOOKS:

1. "Penetration Testing: Hands-on Introduction to Hacking", Georgia Weidman, 1st Edition, No Starch Press.
2. The Pen Tester Blueprint-Starting a Career as an Ethical Hacker ", L. Wylie, Kim Crawly, 1st Edition, Wiley Publications.

DIGITAL FORENSICS

B.Tech Cyber Security (Minor) III Year II Sem. **L T P C**

3 0 0 3

Pre-Requisites: Cybercrime and Information Warfare, Computer Networks

Course Objectives:

1. provides an in-depth study of the rapidly changing and fascinating field of computer forensics.
2. Combines both the technical expertise and the knowledge required to investigate, detect and prevent digital crimes.
3. Knowledge on digital forensics legislations, digital crime, forensics processes and procedures, data acquisition and validation, e-discovery tools
4. E-evidence collection and preservation, investigating operating systems and file systems, network forensics, art of steganography and mobile device forensics

Course Outcomes: On completion of the course the student should be able to

1. Understand relevant legislation and codes of ethics.
2. Computer forensics and digital detective and various processes, policies and procedures.
3. E-discovery, guidelines and standards, E-evidence, tools and environment.
4. Email and web forensics and network forensics.

UNIT - I

Digital Forensics Science: Forensics science, computer forensics, and digital forensics.

Computer Crime: Criminalistics as it relates to the investigative process, analysis of cyber criminalistics area, holistic approach to cyber-forensics

UNIT - II

Cyber Crime Scene Analysis:

Discuss the various court orders etc., methods to search and seizure electronic evidence, retrieved and un-retrieved communications, Discuss the importance of understanding what court documents would be required for a criminal investigation.

UNIT - III

Evidence Management & Presentation:

Create and manage shared folders using operating system, importance of the forensic mindset, define the workload of law enforcement, Explain what the normal case would look like, Define who should be notified of a crime, parts of gathering evidence, Define and apply probable cause.

UNIT - IV

Computer Forensics: Prepare a case, Begin an investigation, Understand computer forensics workstations and software, Conduct an investigation, Complete a case, Critique a case,

Network Forensics: open-source security tools for network forensic analysis, requirements for preservation of network data.

UNIT - V

Mobile Forensics: mobile forensics techniques, mobile forensics tools.

Legal Aspects of Digital Forensics: IT Act 2000, amendment of IT Act 2008.

Recent trends in mobile forensic technique and methods to search and seizure electronic evidence

TEXT BOOKS:

1. John Sammons, The Basics of Digital Forensics, Elsevier
2. John Vacca, Computer Forensics: Computer Crime Scene Investigation, Laxmi Publications

REFERENCES:

1. William Oettinger, Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence, Packt Publishing; 1st edition (30 April 2020), ISBN : 1838648178.
2. Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar, Cybercrime and Digital Forensics: An Introduction, Routledge.

VULNERABILITY ASSESSMENT & PENETRATION TESTING LAB

B.Tech Cyber Security (Minor) III Year II Sem

L	T	P	C
0	0	2	1

Course Objectives:

- Learning Penetration Testing methodologies
- Monitoring the network traffic
- To understand the host and services discovery

Course Outcomes:

- Design for monitoring network traffic.
- Perform different penetration testing methods.
- Design different types of vulnerabilities scanning.
- Understand web application assessment.

List of Experiments:

1. Implement Monitoring of Network Traffic using
    a. wireshark
    b. tcpdump
    c. Nagios
    d. solarwinds
2. Implement Host & Services Discovery using Nmap, massscan.
3. Implement Vulnerability Scanning using OpenVAS, Zapproxy, SQLmap.
4. Implement Internal Penetration Testing.
    a. Mapping
    b. Scanning
    c. Gaining access through CVE's
    d. Sniffing POP3/FTP/Telnet Passwords
    e. ARP Poisoning
    f. DNS Poisoning
5. Implement External Penetration Testing.
    a. Evaluating external Infrastructure.
    b. Creating topological map & identifying IP address of target.
    c. Lookup domain registry for IP information.
    d. Examining use of IPV6 at remote location.
6. Implement Vulnerability scanning with Nessus.
7. Implement Vulnerability scanning with openvas.
8. Implement Web application assessment with nikto.
9. Implement Web application assessment with burp suite.
10. Implement Web application assessment with owaspzap,

TEXT BOOKS:

1. " Gray Hat Hacking-The Ethical Hackers Handbook", Allen Harper, Stephen Sims, Michael Baucom, 3rd Edition, Tata Mc Graw-Hill.
2. " The Web Application Hacker's Handbook-Discovering and Exploiting Security flaws", Dafydd Suttard, Marcus pinto, 1st Edition, Wiley Publishing.

REFERENCE BOOKS:

1. "Penetration Testing: Hands-on Introduction to Hacking", Georgia Weidman, 1st Edition, No Starch Press.
2. " The Pen Tester Blueprint-Starting a Career as an Ethical Hacker ", L. Wylie, Kim Crawly, 1st Edition, Wiley Publications.

DIGITAL FORENSICS LAB

B.Tech Cyber Security (Minor) III Year II Sem

L	T	P	C
0	0	2	1

Course Objectives

1. To provide students with a comprehensive overview of collecting, investigating, preserving, and presenting evidence of cybercrime left in digital storage devices, emails, browsers, mobile devices using different Forensics tools
2. To Understand file system basics and where hidden files may lie on the disk, as well as how to extract the data and preserve it for analysis.
3. Understand some of the tools of e-discovery.
4. To understand the network analysis, Registry analysis and analyze attacks using different forensics tools

Course Outcomes

1. Learn the importance of a systematic procedure for investigation of data found on digital storage media that might provide evidence of wrong-doing
2. To Learn the file system storage mechanisms and retrieve files in hidden format
3. Learn the use of computer forensics tools used in data analysis.
4. Learn how to find data that may be clear or hidden on a computer disk, find our the open ports for the attackers through network analysis , Registry analysis.

Experiments

1. **Perform email analysis** using the tools like Exchange EDB viewer, MBOX viewer and View user mailboxes and public folders , Filter the mailbox data based on various criteria, Search for particular items in user mailboxes and public folders
2. **Perform Browser history analysis** and get the downloaded content, history saved logins, searches, websites visited etc using Foxton Forensics tool,Dumpzilla .
3. **Perform mobile analysis** in the form of retrieving call logs ,SMS log,all contacts list using the forensics tool like SAFT
4. **Perform Registry analysis** and get boot time logging using process monitor tool
5. **Perform Disk imaging and cloning the** using the X-way Forensics tools
6. **Perform Data Analysis i.e** History about open file and folder, and view folder actions using Listview activity tool
7. **Perform Network analysis** using the Network Miner tool **.**
8. **Perform information for incident response** using the crowd Response tool
9. **Perform File type detection using** Autopsy tool
10. **Perform Memory capture and analysis** using the Live RAM capture or any forensic tool

Text Books:

1. Real Digital Forensics for Handheld Devices , E. P. Dorothy, Auerbach Publications, 2013.
2. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, J. Sammons, Syngress Publishing, 2012.

References:

1. Handbook of Digital Forensics and Investigation, E. Casey, Academic Press, 2010
2. Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides, C. H. Malin, E. Casey and J. M. Aquilina, Syngress, 2012
3. The Best Damn Cybercrime and Digital Forensics Book Period, J. Wiles and A.Reyes, Syngress, 2007.

SECURITY INCIDENT AND RESPONSE MANAGEMENT

B.Tech Cyber Security (Minor) IV Year I Sem. **L T P C**

3 0 0 3

Prerequisites:

- Knowledge of information security and applied cryptography.
- Knowledge of Operating Systems.

Course Objectives:

- Give an introduction to the preparation of inevitable incidents, incident detection and characterization.
- To get exposure to live data collection and forensic duplication.
- To gain knowledge on data collection in Windows, Unix and Mac OS Systems.

Course Outcomes:

- Learn how to handle the incident response management.
- Perform live data collection and forensic duplication.
- Identify network evidence.
- Analyze data to carry out an investigation.
- Knowledge on investigation on Mac and Windows OS systems

UNIT-I

Introduction: Preparing for the inevitable incident: Real-world incident, IR management incident handbook, Pre-incident preparation, preparing the Organization for Incident Response, Preparing the IR team, preparing the Infrastructure for Incident Response.

Incident Detection and Characterization: Getting the investigation started on the right foot, collecting initial facts, Maintenance of Case Notes, Understanding Investigative Priorities.

Discovering the scope of Incident: Examining initial data, Gathering and reviewing preliminary evidence, determining a course of action, Customer data loss scenario, automated clearing fraud scenario.

UNIT-II

Data Collection: Live Data Collection: When to perform live response, Selecting a live response tool, what to collect, collection best practices, Live data collection on Microsoft Windows Systems, Live Data Collection on Unix-based Systems.

Forensic Duplication: Forensic Image Formats, Traditional duplication, live system duplication, Duplication of Enterprise Assets.

UNIT-III

Network Evidence: The case for network monitoring, Types for network monitoring, Setting up a Network Monitoring System, Network Data, Analysis, Collect Logs Generated from Network Events.

Enterprise Services: Network Infrastructure Services, Enterprise Management Applications, Web servers, Database Servers.

UNIT-IV

Data Analysis: Analysis Methodology: Define Objectives Know your data, Access your data, Analyze your data, Evaluate Results.

Investigating Windows Systems: NTFS and File System analysis, prefetch, Event logs, Scheduled Tasks, The Windows Registry, Other Artifacts of Interactive Sessions, Memory Forensics, Alternative Persistence Mechanisms.

UNIT-V

Investigating Mac OS X Systems: HFS and File System Analysis, Core Operating Systems data. **Investigating Applications**: What is Application Data? Where is application data stored? General Investigation methods, Web Browser, Email Clients, Instant Message Clients.

TEXT BOOK:

1. “Incident Response and Computer Forensics”, Jason T. Luttgens, Mathew Pepe and Kevin Mandia, 3rd Edition, Tata McGraw-Hill Education.

REFERENCE BOOKS:

1. “Cyber Security Incident Response-How to Contain, Eradicate, and Recover from Incidents”, Eric. C. Thompson, Apress.
2. “The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk”, N.K. McCarthy, Tata McGraw-Hill.

MOBILE SECURITY

B.Tech Cyber Security (Minor) IV Year I Sem. **L T P C**

3 0 0 3

Course Objectives: This course provides a thorough understanding of mobile platforms, including attack surfaces, risk landscape & more.

Course Outcomes:

1. Understand common mobile application security vulnerabilities
2. Define the security controls of multiple mobile operating systems
3. Understand and analyze Bluetooth technology
4. understand and analyze overview of SMS security and Enterprise security

UNIT-I

Top Mobile Issues and Development Strategies: Top Issues Facing Mobile Devices, Physical Security , Secure Data Storage (on Disk), Strong Authentication with Poor Keyboards , Multiple-User Support with Security, Safe Browsing Environment , Secure Operating Systems, Application Isolation, Information Disclosure, Virus, Worms, Trojans, Spyware, and Malware , Difficult Patching/Update Process, Strict Use and Enforcement of SSL, Phishing , Cross-Site Request Forgery (CSRF), Location Privacy/Security, Insecure Device Drivers, Multi Factor Authentication, Tips for Secure Mobile Application Development .

UNIT-II

WAP and Mobile HTML Security WAP and Mobile HTML Basics , Authentication on WAP/Mobile HTML Sites , Encryption, Application Attacks on Mobile HTML Sites ,Cross-Site Scripting , SQL Injection , Cross-Site Request Forgery , HTTP Redirects , Phishing , Session Fixation , Non-SSL Login , WAP and Mobile Browser Weaknesses , Lack of HTTPOnly Flag Support , Lack of SECURE Flag Support , Handling Browser Cache , WAP Limitations.

UNIT-III

Bluetooth Security Overview of the Technology , History and Standards , Common Uses , Alternatives , Future, Bluetooth Technical Architecture , Radio Operation and Frequency, Bluetooth Network Topology , Device Identification , Modes of Operation , Bluetooth Stack ,Bluetooth Profiles, Bluetooth Security Features , Pairing , Traditional Security Services in Bluetooth, Security “Non-Features” , Threats to Bluetooth Devices and Networks, Bluetooth Vulnerabilities, Bluetooth Versions Prior to v1.2, Bluetooth Versions Prior to v2.1. Security for 1g Wi-Fi Applications, Security for 2g Wi-Fi Applications, Recent Security Schemes for Wi-Fi Applications

UNIT-IV

SMS Security Overview of Short Message Service, Overview of Multimedia Messaging Service, Wireless Application Protocol (WAP), Protocol Attacks, Abusing Legitimate Functionality, Attacking Protocol Implementations, Application Attacks, iPhone Safari, Windows Mobile MMS, Motorola RAZR JPG Overflow, Walkthroughs, Sending PDUs,Converting XML to WBXML.

UNIT-V

Enterprise Security on the Mobile OS Device Security Options, PIN, Remote, Secure Local Storage, Apple iPhone and Keychain, Security Policy Enforcement, Encryption, Full Disk Encryption, E-mail Encryption, File Encryption, Application Sandboxing, Signing, and Permissions, Application Sandboxing, Application Signing, Permissions, Buffer Overflow Protection,Windows Mobile, iPhone, Android,BlackBerry, Security Feature Summary.

Textbook:

1. Mobile Application Security, HimanshuDwivedi, Chris Clark, David Thiel, TATA McGRAW-Hill.

References:

1. Mobile and Wireless Network Security and Privacy, Kami S.Makki, et al, Springer.
2. Android Security Attacks Defenses, Abhishek Dubey, CRC Press

IOT SECURITY

B.Tech Cyber Security (Minor) IV Year I Sem. **L T P C**

3 0 0 3

Course Objectives

- Understand the fundamentals, various attacks and importance of Security aspects in IoT
- Understand the techniques, protocols and some idea on security towards Gaming models
- Understand the operations of Bitcoin blockchain, crypto-currency as application of blockchain technology
- Understand the essential components of IoT
- Understand security and privacy challenges of IoT

Course Outcomes:

1. Incorporate the best practices learnt to identify the attacks and mitigate the same
2. Adopt the right security techniques and protocols during the design of IoT products
3. Assimilate and apply the skills learnt on ciphers and block chains when appropriate
4. Describe the essential components of IoT
5. Find appropriate security/privacy solutions for IoT

Unit-I

Fundamentals of IoT and Security and its need, Prevent Unauthorized Access to Sensor Data
Block ciphers Introduction to Blockchain, Introduction of IoT devices
IoT Security Requirements ,M2M Security, Message integrity Modeling faults and adversaries Difference among IoT devices, computers, and embedded devices.

Unit-II

IoT and cyber-physical systems RFID Security, Authenticated encryption Byzantine Generals problem sensors and actuators in IoT
IoT security (vulnerabilities, attacks, and countermeasures), Cyber Physical Object Security, , Hash functions Consensus algorithms and their scalability problems Accelerometer, photoresistor, buttons

Unit-III

Security engineering for IoT development Hardware Security, Merkle trees and Elliptic curves digital signatures, verifiable random functions, Zero-knowledge systems motor, LED, vibrator
IoT security lifecycle Front-end System Privacy Protection, Management, Secure IoT Databases
Public-key crypto (PKI), blockchain, the challenges, and solutions, analog signal vs. digital signal

Unit-IV

Data Privacy Networking Function Security Trees signature algorithms proof of work, Proof of stake, Networking in IoT Device/User Authentication in IoT IoT Networking Protocols, Crypto-currencies, alternatives to Bitcoin consensus, Bitcoin scripting language and their use Real-time communication

Unit-V

Introduction to Authentication Techniques Secure IoT Lower Layers, Bitcoin P2P network, Ethereum and Smart Contracts, Bandwidth efficiency
Data Trustworthiness in IoT Secure IoT Higher Layers, Distributed consensus, Smart Contract Languages and verification challenges data analytics in IoT - simple data analyzing methods

TEXT BOOKS:

1. B. Russell and D. Van Duren, “Practical Internet of Things Security,” Packt Publishing, 2016.
2. Fei HU, “Security and Privacy Internet of Things (IoTs): Models, Algorithms and Implementations”, CRC Press, 2016

3. Narayanan et al., “Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction,” Princeton University Press, 2016.

Reference Books.

1. A. Antonopoulos, “Mastering Bitcoin: Unlocking Digital Crypto currencies,” O’Reilly, 2014.
2. T. Alpcan and T. Basar, “Network Security: A Decision and Game-theoretic Approach,” Cambridge University Press,2011.
3. Security and the IoT ecosystem, KPMG International, 2015.
4. Internet of Things: IoT Governance, Privacy and Security Issues” European Research Cluster.
5. Ollie Whitehouse, “Security of Things: An Implementers' Guide to Cyber-Security for Internet of Things Devices and Beyond”, NCC Group, 2014.
6. Josh Thompson, ‘Blockchain: The Blockchain for Beginnings, Guide to Blockchain Technology and Blockchain Programming’, Create Space Independent Publishing Platform, 2017.

BLOCKCHAIN TECHNOLOGY

B.Tech Cyber Security (Minor) IV Year I Sem. **L T P C**

3 0 0 3

Prerequisites:

1. Knowledge in information security and applied cryptography.
2. Knowledge in Computer Networks

Course Objectives:

- To learn the fundamentals of Blockchain and various types of block chain and consensus mechanisms.
- To understand the public block chain system, Private block chain system and consortium blockchain.
- Able to know the security issues of blockchain technology.

Course Outcomes:

- Understanding concepts behind crypto currency
- Applications of smart contracts in decentralized application development
- Understand frameworks related to public, private and hybrid blockchain
- Create blockchain for different application case studies

UNIT - I

Fundamentals of Blockchain: Introduction, Origin of Blockchain, Blockchain Solution, Components of Blockchain, Block in a Blockchain, The Technology and the Future.

Blockchain Types and Consensus Mechanism: Introduction, Decentralization and Distribution, Types of Blockchain, Consensus Protocol.

Cryptocurrency – Bitcoin, Altcoin and Token: Introduction, Bitcoin and the Cryptocurrency, Cryptocurrency Basics, Types of Cryptocurrencies, Cryptocurrency Usage.

UNIT - II

Public Blockchain System: Introduction, Public Blockchain, Popular Public Blockchains, The Bitcoin Blockchain, Ethereum Blockchain.

Smart Contracts: Introduction, Smart Contract, Characteristics of a Smart Contract, Types of Smart Contracts, Types of Oracles, Smart Contracts in Ethereum, Smart Contracts in Industry.

UNIT - III

Private Blockchain System: Introduction, Key Characteristics of Private Blockchain, Need of Private Blockchain, Private Blockchain Examples, Private Blockchain and Open Source, E- commerce Site Example, Various Commands (Instructions) in E-commerce Blockchain, Smart Contract in Private Environment, State Machine, Different Algorithms of Permissioned Blockchain, Byzantine Fault, Multichain.

Consortium Blockchain: Introduction, Key Characteristics of Consortium Blockchain, Need of Consortium Blockchain, Hyperledger Platform, Overview of Ripple, Overview of Corda.

Initial Coin Offering: Introduction, Blockchain Fundraising Methods, Launching an ICO, Investing in an ICO, Pros and Cons of Initial Coin Offering, Successful Initial Coin Offerings, Evolution of ICO, ICO Platforms.

UNIT - IV

Security in Blockchain: Introduction, Security Aspects in Bitcoin, Security and Privacy Challenges of Blockchain in General, Performance and Scalability, Identity Management and Authentication, Regulatory Compliance and Assurance, Safeguarding Blockchain Smart Contract (DApp), Security Aspects in Hyperledger Fabric.

Applications of Blockchain: Introduction, Blockchain in Banking and Finance, Blockchain in Education, Blockchain in Energy, Blockchain in Healthcare, Blockchain in Real-estate, Blockchain In Supply Chain, The Blockchain and IoT. Limitations and Challenges of Blockchain.

UNIT - V

Blockchain Case Studies: Case Study 1 – Retail, Case Study 2 – Banking and Financial Services, Case Study 3 – Healthcare, Case Study 4 – Energy and Utilities.

Blockchain Platform using Python: Introduction, Learn How to Use Python Online Editor, Basic Programming Using Python, Python Packages for Blockchain.

Blockchain platform using Hyperledger Fabric: Introduction, Components of Hyper ledger Fabric Network, Chain codes from Developer.ibm.com, Blockchain Application Using Fabric Java SDK.

TEXT BOOK:

1. "Blockchain Technology", Chandramouli Subramanian, Asha A. George, Abhilasj K A and Meena Karthikeyan, Universities Press.

REFERENCE BOOKS:

1. Michael Juntao Yuan, Building Blockchain Apps, Pearson, India.
2. Blockchain Blueprint for Economy, Melanie Swan, SPD O'reilly.
3. Blockchain for Business, Jai Singh Arun, Jerry Cuomo, Nitin Gaur, Pearson.

AUTHENTICATION TECHNIQUES

B.Tech Cyber Security (Minor) IV Year I Sem. **L T P C**

3 0 0 3

Course Objectives

Knowledge on concept of authentication types, protocols, physical identification and various authentication algorithms

Course Outcomes

1. Understand different types of authentication techniques
2. Understand text based and voice based authentication techniques
3. Understand significance of authentication algorithms and its standards
4. Apply various authentication protocols in multi-server environment and their representation

Unit-1:

Definition of Authentication, Identification/verification, Stages and steps of authentication, Authentication Entity : User, Device and Application; Authentication attributes: Source, Location, Path, Time duration etc.; Authentication Types : Direct / Indirect, One Way / Mutual, On demand/ Periodic/ Dynamic/Continuous authentication, Assisted/Automatic; 3 Factors of authentication; Passwords, Generation of passwords of varied length and of mixed type, OTP, passwords generation using entity identity credentials; Secure capture, processing, storage, verification and retrieval of passwords;

Unit-2:

Physical identification using smart cards, remote control device, proximity sensors, surveillance camera, authentication in Card present / Card Not Present transactions as ATM/ PoS Device, mobile phone, wearable deviceand IoT device based authentication; single sign- on; Symmetric Key Generation, Key Establishment, Key Agreement Protocols;

Unit-3:

Biometrics – photo, face, iris, retinal, handwriting, signature, fingerprint, palm print, hand geometry, voice – Text based and text independent voice authentication, style of talking, walking, writing, keystrokes, gait etc. multi-modal biometrics.

Unit-4:

Matching algorithms, Patterns analysis, errors, performance measures, ROC Curve; Authentication Standards – International, UIDAI Standard. Kerberos, X.509 Authentication Service, Public Key Infrastructure, Scanners and Software; Web Authentication Methods: Http based, Token Based, OAuthand API.

Unit-5:

User authentication protocols in multi-server environment, BAN Logic, Representation of authentication protocols using BAN Logic, Random Oracle Model, Scyther Tools, Proverif tool, Chebyshev Chaotic Map, Fuzzy Extractor, Fuzzy Extractor Map, Bloom Filter, LU Decomposition based User Authentication, Blockchain based authentication.

Text Books:

1. Protocols for Authentication and Key Establishment, Colin Boyd and Anish Mathuria, springer, 2021
2. Guide to Biometrics, Ruud M. Bolle, Sharath Pankanti, Nalini K. Ratha, Andrew W. Senior, Jonathan H. Connell, Springer 2009.

References:

1. Digital Image Processing using MATLAB, Rafael C. Gonzalez, Richard Eugene Woods, 2nd Edition, Tata McGraw-Hill Education 2010.
2. Biometric System and Data Analysis: Design, Evaluation, and data Mining, Ted Dunstone and Neil Yager, Springer.
3. Biometrics Technologies and verification Systems, John Vacca, , Elsevier Inc. 2007.
4. Pattern Classification, Richard O. Duda, David G.Stork, Peter E. Hart, Wiley 2007.

CLOUD SECURITY

B.Tech Cyber Security (Minor) IV Year I Sem. **L T P C**

3 0 0 3

Pre-requisites: Computer Networks, Cryptography and Network Security, Cloud Computing.

Course Objectives

- To understand the fundamentals concepts of cloud computing.
- To understand the cloud security and privacy issues.
- To understand the Threat Model and Cloud Attacks
- To understand the Data Security and Storage
- To analyze Security Management in the Cloud.

Course Outcome

1. Ability to acquire the knowledge on fundamentals concepts of cloud computing.
2. Able to distinguish the various cloud security and privacy issues.
3. Able to analyze the various threats and Attack tools
4. Able to understand the Data Security and Storage
5. Able to analyze the Security Management in the Cloud.

Unit - I

Overview of Cloud Computing: Introduction, Definitions and Characteristics, Cloud Service Models, Cloud Deployment Models, Cloud Service Platforms, Challenges Ahead.

Introduction to Cloud Security: Introduction, Cloud Security Concepts, CSA Cloud Reference Model, NIST Cloud Reference Model, NIST Cloud Reference Model.

Note: Laboratory practice will be imparted with the help of relevant case studies as and when required.

Unit - II

Cloud Security and Privacy Issues: Introduction, Cloud Security Goals/Concepts, Cloud Security Issues, Security Requirements for Privacy, Privacy Issues in Cloud.

Infrastructure Security: The Network Level, the Host Level,the Application Level, SaaS Application Security, PaaS Application Security, IaaS Application Security.

Note: Laboratory practice will be imparted with the help of relevant case studies as and when required.

Unit - III

Threat Model and Cloud Attacks: Introduction, Threat Model- Type of attack entities, Attack surfaces with attack scenarios, A Taxonomy of Attacks, Attack Tools-Network-level attack tools, VM-level attack tools, VMM attack tools, Security Tools, VMM security tools.

Note: Laboratory practice will be imparted with the help of relevant case studies as and when required.

Unit - IV

Information Security Basic Concepts, an Example of a Security Attack, Cloud Software Security Requirements, Rising Security Threats. **Data Security and Storage:** Aspects of Data Security, Data Security Mitigation, Provider Data and Its Security.

Note: Laboratory practice will be imparted with the help of relevant case studies as and when required.

Unit - V

Evolution of Security Considerations, Security Concerns of Cloud Operating Models, Identity Authentication, Secure Transmissions, Secure Storage and Computation, Security Using Encryption Keys, Challenges of Using Standard Security Algorithms, Variations and Special Cases for Security Issues with Cloud Computing, Side Channel Security Attacks in the Cloud

Security Management in the Cloud- Security Management Standards, Availability Management, Access Control, Security Vulnerability, Patch, and Configuration Management.

Note: Laboratory practice will be imparted with the help of relevant case studies as and when required.

Text Books:

1. Cloud Security Attacks, Techniques, Tools, and Challenges by Preeti Mishra, Emmanuel S Pilli, Jaipur R C Joshi Graphic Era, 1st Edition published 2022 by CRC press.
2. Cloud Computing with Security Concepts and Practices Second Edition by Naresh Kumar Sehgal Pramod Chandra, P. Bhatt John M. Acken, 2nd Edition Springer nature Switzerland AG 2020.
3. Cloud Security and Privacy by Tim Mather, Subra Kumaraswamy, and Shahed Lati First Edition, September 2019.

Reference Books:

1. Essentials of Cloud Computing by K. Chandrasekaran Special Indian Edition CRC press.
2. Cloud Computing Principles and Paradigms by Rajkumar Buyya, John Wiley.