Department of Computer Science and Engineering

B.Tech. with Minor Degree Program in Cyber Security

B.Tech. with Minor Degree Program in Cyber Security

Course Structure (2021-22)

(Applicable for 2019-2023 Batch-R19 Syllabus)

(Offered by JNTUH, Hyderabad)

Year/Semester	**Theory**	**Laboratory (3 Hours, 1.5 Credits)**	**Total Credits**
III - I Semester	Principles of Information Security (3 Credits, 3 Hours)	Principles of Information Security Lab	4.5
III - II Semester	Foundations of Cyber Security (4 Credits, 4 Hours)	--	4
IV - I Semester	(Either online through MOOCS or off-line Class) Ethical Hacking **OR** Digital Forensics (3 Credits, 3 Hours)	(The corresponding Lab) Ethical Hacking Lab **OR** Digital Forensics Lab	4.5
IV - II Semester	**Any one of the following subjects:** (3 Credits, 3 Hours) 1. Security Incident & Response Management 2. Mobile Security 3. IoT Security 4. Blockchain Technologies 5. Authentication Techniques Cloud Security	--	3
IV-II Semester	Mini Project	--	2
Total Credits			**18**

B.Tech. with Minor Degree Program in Cyber Security

Course Structure (2021-22)

(Applicable for 2019-2023 Batch-R19 Syllabus)

III YEAR I & II SEMESTER

Year/Semester	Theory	Laboratory	Total Credits
III - I Semester	Principles of Information Security(3 Credits, 3 Hours)	Principles of Informatio Security Lab (3 Hours, 1.5Credits)	4.5
III - II Semester	Foundations of Cyber Security(3 Credits, 3 Hours)	Cyber Security Lab (2 Hours,1 Credit)	4
Total Credits			**8.5**

Department of Computer Science and Engineering

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

III Year-I Semester **L T P C**

Principles of Information Security **3 0 0 3**

Prerequisites

1. A course on "Mathematics"

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.
5. To apply algorithms used for message integrity and authentication.

Outcomes

1. Demonstrate the knowledge of Computer networks, cryptography, information security concepts and applications.
2. 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 stander (DES), advanced encryption standerd (AES)

UNIT III

Mathematics of cryptography: primes, primality testing, factorization, Chinese reminder 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, Person 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.

Department of Computer Science and Engineering

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

III Year-I Semester **L T P C**

Principles of Information Security Lab **0 0 3 1.5**

Prerequisites

A course on "Mathematics"

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 substitution ciphers.
2. Caeser cipher
3. Play fair cipher
4. Hill cipher
5. Write a program to implement the DES algorithm.
6. Write a program to implement RSA algorithm.
7. Calculate the message digest of a text using the SHA-1 algorithm.
8. Working with sniffers for monitoring network communication (wireshark)
9. Configuring S/MIME for email communication.
10. Using Snort, perform real time traffic analysis and packet logging.

Text Books:

1. "Cryptography and Network Security" by William Stallings 3rd Edition, Pearson Education.
2. "Applied Cryptography" by Bruce Schneier.

Reference Book:

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

Department of Computer Science and Engineering

B.Tech. with Minor program in Cyber Security

(Offered by JNTUH, Hyderabad)

III Year-I Semester **L T P C**

Principles of Information Security **3 0 0 3**

Prerequisites

1.A course on "Mathematics"

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.
5. To apply algorithms used for message integrity and authentication.

Outcomes

1.Demonstrate the knowledge of Computer networks, cryptography, information security concepts and applications.
2. 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 stander(DES), advanced encryption standerd(AES)

UNIT III

Mathematics of cryptography: primes, primality testing, factorization, Chinese reminder 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, Person 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.

Department of Computer Science and Engineering

B.Tech. with Minor program in Cyber Security

(Offered by JNTUH, Hyderabad)

III Year-I Semester **L T P C**

Principles of Information Security Lab **0 0 3 1.5**

Prerequisites

A course on "Mathematics"

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 substitution ciphers.

2. Caeser cipher

3. Play fair cipher

4. Hill cipher

5. Write a program to implement the DES algorithm.

6. Write a program to implement RSA algorithm.

7. Calculate the message digest of a text using the SHA-1 algorithm.

8. Working with sniffers for monitoring network communication (wireshark)

9. Configuring S/MIME for email communication.

10. Using Snort, perform real time traffic analysis and packet logging.

Text Books:

1."Cryptography and Network Security" by William Stallings 3rd Edition, Pearson Education.
2. "Applied Cryptography" by Bruce Schneier.

Reference Book:

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

Department of Computer Science and Engineering

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

III Year-II Semester **L T P C**

Foundations of Cyber Security **4 0 0 4**

Pre-requisites:

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

Course Objectives:

1. To introduce security attacks.
2. To get an exposure to malwares.
3. To gain knowledge on Intrusion detection & prevention systems.

Course Outcomes: Students will learn the fundamental concepts required in the field of cyber security.

UNIT – I

Overview: Computer Security Concepts, Threats, Attacks, and Assets, Security Functional Requirements, Fundamental Security Design Principles, Attack Surfaces and Attack Trees, Computer Security Strategy.

Access Control: Access Control Principles, Subjects, Objects, and Access Rights, Discretionary Access Control, Example: UNIX File Access Control, Role-Based Access Control, Attribute-Based Access Control, Identity, Credential, and Access Management, Trust Frameworks, Case Study: RBAC System for a Bank.

UNIT II

Malicious Software: Types of Malicious Software (Malware), Advanced Persistent Threat, Propagation—Infected Content—Viruses, Propagation—Vulnerability Exploit—Worms, Propagation— Social Engineering—Spam E-Mail, Trojans, Payload—System Corruption, Payload—Attack Agent— Zombie, Bots, Payload—Information Theft—Key loggers, Phishing, Spyware, Payload—Stealthing— Backdoors, Rootkits, Counter measures.

Denial-of-Service Attacks: Denial-of-Service Attacks, Flooding Attacks, Distributed Denial-of-Service Attacks, Application-Based Bandwidth Attacks, Reflector and Amplifier Attacks, Defences Against Denial-of-Service Attacks, Responding to a Denial-of-Service Attack.

Buffer Overflow: Stack Overflows, Defending Against Buffer Overflows, Other Forms of Overflow Attacks.

UNIT - III

Intrusion Detection: Intruders, Intrusion Detection, Analysis Approaches, Host-Based Intrusion Detection, Network-Based Intrusion Detection, Distributed or Hybrid Intrusion Detection, Intrusion Detection Exchange Format, Honeypots, Example System: Snort.

Firewalls and Intrusion Prevention Systems: The Need for Firewalls, Firewall Characteristics and Access Policy, Types of Firewalls, Firewall Basing, Firewall Location and Configurations, Intrusion Prevention Systems, Example: Unified Threat Management Products.

UNIT - IV

Software Security: Software Security Issues, Handling Program Input, Writing Safe Program Code, Interacting with the Operating System and Other Programs, Handling Program Output.
Physical and Infrastructure Security: Overview, Physical Security Threats, Physical Security Prevention and Mitigation Measures, Recovery from Physical Security Breaches, Example: A Corporate Physical Security Policy, Integration of Physical and Logical Security.

UNIT - V

Human Resources Security: Security Awareness, Training, and Education, Employment Practices and Policies, E-Mail and Internet Use Policies, Computer Security Incident Response Teams.
Legal and Ethical Aspects: Cybercrime and Computer Crime, Intellectual Property, Privacy, Ethical Issues.

TEXT BOOK:

1. William Stallings, "Computer Security: Principles and Practice", Prentice Hall. Prentice Hall; 2014.

REFERENCE BOOKS:

1. Ankit Fadia, "The ethical hacking guide to corporate security", McMillan India.
2. G. McGraw, "Software Security: Building Security In", Addison Wesley, 2006.

Department of Computer Science and Engineering

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

III Year-II Semester	**L**	**T**	**P**	**C**
Cyber Security Lab	**0**	**0**	**2**	**1**

List of Experiments:

1. Implement the following UNIX commands.

   (a) cat (b) ls (c) chmod (d)mkdir (e) rmdir

2. Write a shell script that displays a list of all the files in the current directory to which the user has read, write and execute permissions.
3. Write a shell script to list all of the directory files in a directory.
4. Write a C program to create a child process and allow the parent to display "parent" and the child to display "child" on the screen.
5. Write a C program to create

   (a) Zombie process (b) Orphan process

6. Write a code to demonstrate Denial of Service (DoS) attacks.
7. Create a social networking website login page using phishing techniques.
8. Write a script or code to demonstrate SQL injection attacks.
9. Demonstrate intrusion detection system (ids) using any tool.
10 (a) Study "How to make strong passwords" and "passwords cracking techniques".

   (b) Study the steps how to hack a strong password.

Department of Computer Science and Engineering

B.Tech. with Minor program in Cyber Security

(Offered by JNTUH, Hyderabad)

III Year-II Semester **L T P C**

Foundations of Cyber Security **4 0 0 4**

Pre-requisites:

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

Course Objectives:

1. To introduce security attacks.
2. To get an exposure to malwares.
3. To gain knowledge on Intrusion detection & prevention systems.

Course Outcomes: Students will learn the fundamental concepts required in the field of cyber security.

UNIT – I

Overview: Computer Security Concepts, Threats, Attacks, and Assets, Security Functional Requirements, Fundamental Security Design Principles, Attack Surfaces and Attack Trees, Computer Security Strategy.

Access Control: Access Control Principles, Subjects, Objects, and Access Rights, Discretionary Access Control, Example: UNIX File Access Control, Role-Based Access Control, Attribute-Based Access Control, Identity, Credential, and Access Management, Trust Frameworks, Case Study: RBAC System for a Bank.

UNIT **II**

Malicious Software: Types of Malicious Software (Malware), Advanced Persistent Threat, Propagation—Infected Content—Viruses, Propagation—Vulnerability Exploit—Worms, Propagation— Social Engineering—Spam E-Mail,Trojans , Payload—System Corruption, Payload—Attack Agent— Zombie, Bots, Payload—Information Theft—Keyloggers, Phishing, Spyware, Payload—Stealthing— Backdoors, Rootkits, Counter measures.

Denial-of-Service Attacks: Denial-of-Service Attacks, Flooding Attacks, Distributed Denial-of-Service Attacks, Application-Based Bandwidth Attacks, Reflector and Amplifier Attacks, Defenses Against Denial-of-Service Attacks, Responding to a Denial-of-Service Attack.

Buffer Overflow: Stack Overflows, Defending Against Buffer Overflows, Other Forms of Overflow Attacks.

UNIT - III

Intrusion Detection: Intruders, Intrusion Detection, Analysis Approaches, Host-Based Intrusion Detection, Network-Based Intrusion Detection, Distributed or Hybrid Intrusion Detection, Intrusion Detection Exchange Format, Honeypots, Example System: Snort.

Firewalls and Intrusion Prevention Systems: The Need for Firewalls, Firewall Characteristics and Access Policy, Types of Firewalls, Firewall Basing, Firewall Location and Configurations, Intrusion Prevention Systems, Example: Unified Threat Management Products.

UNIT - IV

Software Security: Software Security Issues, Handling Program Input, Writing Safe Program Code, Interacting with the Operating System and Other Programs, Handling Program Output.
Physical and Infrastructure Security: Overview, Physical Security Threats, Physical Security Prevention and Mitigation Measures, Recovery from Physical Security Breaches, Example: A Corporate Physical Security Policy, Integration of Physical and Logical Security.

UNIT - V

Human Resources Security: Security Awareness, Training, and Education, Employment Practices and Policies, E-Mail and Internet Use Policies, Computer Security Incident Response Teams.
Legal and Ethical Aspects: Cybercrime and Computer Crime, Intellectual Property, Privacy, Ethical Issues.

TEXT BOOK:

1. William Stallings, "Computer Security: Principles and Practice", Prentice Hall. Prentice Hall; 2014.

REFERENCE BOOKS:

1. Ankit Fadia, "The ethical hacking guide to corporate security", McMillan India.
2. G. McGraw, "Software Security: Building Security In", Addison Wesley, 2006.

IV YEAR & II YEAR SEMESTER

Year/Semester	**Theory**	**Laboratory (3 Hours, 1.5 Credits)**	**Total Credits**
IV - I Semester	(Either online through MOOCS or off-line Class) Ethical Hacking **OR** Digital Forensics (3 Credits, 3 Hours)	(The corresponding Lab) Ethical Hacking Lab **OR** Digital Forensics Lab	4.5
IV - II Semester	**Any one of the following subjects:** (3 Credits, 3 Hours) 1. Security Incident & Response Management 2. Mobile Security 3. IoT Security 4. Blockchain Technologies 5. Authentication Techniques Cloud Security	--	3
IV-II Semester	Mini Project	--	2
Total Credits			**9.5**
Grand Total Credits			**18**

ETHICAL HACKING

B.Tech. IV Year I Sem. **L T P C**
3 - - 3

Course Objectives:

- The aim of the course is to introduce the methodologies and framework of ethical hacking for enhancing the security.
- The course includes-Impacts of Hacking; Types of Hackers; Information Security Models;
- Information Security Program; Business Perspective; Planning a Controlled Attack; Framework of Steps (Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Deliverable and Integration)

Course Outcomes:

- Gain the knowledge of the use and availability of tools to support an ethical hack
- Gain the knowledge of interpreting the results of a controlled attack
- Understand the role of politics, inherent and imposed limitations and metrics for planning of a test
- Comprehend the dangers associated with penetration testing

UNIT- I

Introduction: Hacking Impacts, The Hacker
Framework: Planning the test, Sound Operations, Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Final Analysis, Deliverable, Integration. Information Security Models: Computer Security, Network Security, Service Security, Application Security, Security Architecture. **Information Security Program**: The Process of Information Security, Component Parts of Information Security Program, Risk Analysis and Ethical Hacking.

UNIT - II

The Business Perspective: Business Objectives, Security Policy, Previous Test Results, Business Challenges. **Planning for a Controlled Attack:** Inherent Limitations, Imposed Limitations, timing is Everything, Attack Type, Source Point, Required Knowledge, Multi-Phased Attacks, Teaming and Attack Structure, Engagement Planner, The Right Security Consultant, The Tester, Logistics, Intermediates, Law Enforcement.

UNIT - III

Preparing for a Hack: Technical Preparation, Managing the Engagement. Reconnaissance: Social Engineering, Physical Security, Internet Reconnaissance.

UNIT - IV

Enumeration: Enumeration Techniques, Soft Objective, Looking Around or Attack, Elements of Enumeration, Preparing for the Next Phase. **Exploitation:** Intutive Testing, Evasion, Threads and Groups, Operating Systems, Password Crackers, RootKits, applications, Wardialing, Network, Services and Areas of Concern.

UNIT - V

Deliverable: The Deliverable, The Document, Overal Structure, Aligning Findings, Presentation. **Integration:** Integrating the Results, Integration Summary, Mitigation, Defense Planning, Incident Management, Security Policy, Conclusion.

TEXT BOOK:

1. James S. Tiller, “The Ethical Hack: A Framework for Business Value Penetration Testing”,

Auerbach Publications, CRC Press.

REFERENCE BOOKS:

1. EC-Council, "Ethical Hacking and Countermeasures Attack Phases", Cengage Learning.
2. Michael Simpson, Kent Backman, James Corley, "Hands-On Ethical Hacking and Network Defense", Cengage Learning.

DIGITAL FORENSICS

B.Tech. IV Year I Sem. **L T P C**
3 - - 3

Course Objective

- To understand the basic digital forensics and techniques for conducting the forensic examination on different digital devices.
- To understand how to examine digital evidences such as the data acquisition, identification analysis.

Course Outcomes

- Know how to apply forensic analysis tools to recover important evidence for identifying computer crime.
- To be well-trained as next-generation computer crime investigators.
- Knowledge on Forensics acquisition tools.
- Knowledge on Processing crimes and Scenes.
- Knowledge on validating and testing forensic software's.

UNIT -I

Computer Forensics Fundamentals, Benefits of Forensics, Computer Crimes, Computer Forensics Evidence and Courts, Legal Concerns and Private issues.

UNIT- II

Understanding Computing Investigations – Procedure for corporate High-Tech investigations, understanding data recovery work station and software, conducting and investigations.

UNIT-III

Data acquisition- understanding storage formats and digital evidence, determining the best acquisition method, acquisition tools, validating data acquisitions, performing RAID data acquisitions, remote network acquisition tools, other forensics acquisitions tools.

UNIT-IV

Processing crimes and incident scenes, securing a computer incident or crime, seizing digital evidence at scene, storing digital evidence, obtaining digital hash, reviewing case.

UNIT-V

Current computer forensics tools- software, hardware tools, validating and testing forensic software, addressing data-hiding techniques, performing remote acquisitions, e-mail investigations- investigating email crime and violations, understanding e-mail servers, specialized e-mail forensics tool.

TEXT BOOKS:

1. Warren G. Kruse II and Jay G. Heiser, "Computer Forensics: Incident Response Essentials", Addison Wesley, 2002.
2. Nelson, B, Phillips, A, Enfinger, F, Stuart, C., "Guide to Computer Forensics and Investigations, 2nd ed., Thomson Course Technology, 2006, ISBN: 0-619-21706-5.

REFERENCES:

1. Vacca, J, Computer Forensics, Computer Crime Scene Investigation, 2nd Ed, Charles River Media, 2005, ISBN: 1-58450-389.

ETHICAL HACKING LAB

B.Tech. IV Year I Sem.

L	T	P	C
-	-	3	1.5

Course Objectives

- The aim of the course is to introduce the methodologies framework tools of ethical hacking to get awareness in enhancing the security
- To get knowledge on various attacks and their detection

Course Outcomes

- Gain the knowledge of the use and availability of tools to support an ethical hack
- Gain the knowledge of interpreting the results of a controlled attack

List of Experiments

1. Install rootkits and study variety of options
2. Study of Techniques uses for Web Based Password Capturing.
3. Install jcrypt tool (or any other equivalent) and demonstrate Asymmetric, Symmetric Crypto algorithm, Hash and Digital/PKI signatures studied in theory Network Security And Management
4. Implement Passive scanning, active scanning, session hizaking, cookies extraction using
5. Burp suit tool
6. Use a cryptographic algorithm to encrypt and decrypt passwords.
7. Use google and whois for reconnaissance.
8. Use NMAP scanner to perform port scanning of various forms.
9. Perform ARP poisoning for windows.
10. Simulate cross-site scripting attack.
11. Session impersonation using Firefox and Tamper Data add-on.
12. Create a simple Keylogger using python.
13. Using Metasploit to exploit using Linux.

DIGITAL FORENSICS LAB

B.Tech. IV Year I Sem. **L T P C**
- - 3 1.5

Course Objectives:

- 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.
- 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.
- Understand some of the tools of e-discovery.
- To understand the network analysis, Registry analysis and analyze attacks using different
- forensics tools.

Course Outcomes:

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

List of 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 Lastview 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, Auerback Publications, 2013.
2. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, J. Sammons, Syngress Publishing, 2012.

REFERENCE BOOKS:

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. IV Year II Sem. **L T P C**
3 - - 3

Prerequisites:
- Knowledge in information security and applied cryptography.

Course Objectives:
1. Introduce preparation of inevitable incident and incident detection and characterization.
2. To get an exposure to live data collection, Forensic duplication.
3. To gain knowledge on data analysis including Windows and Mac OS Systems.

Course Outcomes:
1. Learn how to handle the incident response management.
2. Perform live data collection and forensic duplication.
3. Identify network evidence.
4. Analyze data to carry out investigation.

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, Analyse 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 BOOKS:

1. "Incident Response and Computer Forensics", Jason T. Luttgens, Mathew Pepe and Kevin Mandia, 3rd Edition, Tata McGraw-Hill Education.
2. "Cyber Security Incident Response-How to Contain, Eradicate, and Recover from Incidents", Eric. C. Thompson, Apress.

REFERENCE BOOKS:

1. "The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk", N.K. McCarthy, Tata McGraw-Hill.

MOBILE SECURITY

B.Tech. IV Year II Sem. **L T P C**
3 - - 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.

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, 346 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.

TEXT BOOK:

1. Mobile Application Security, Himanshu Dwivedi, Chris Clark, David Thiel, TATA McGraw Hill.

REFERENCE BOOKS:

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. IV Year II Sem. **L T P C**
3 - - 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:

- Incorporate the best practices learnt to identify the attacks and mitigate the same.
- Adopt the right security techniques and protocols during the design of IoT products.
- Assimilate and apply the skills learnt on ciphers and block chains when appropriate.
- Describe the essential components of IoT.
- 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. FeiHU, "Security and Privacy in 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. Antonopoulos, "Mastering Bitcoin: Unlocking Digital Cryptocurrencies," 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" by 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. IV Year II Sem. **L T P C**
3 - - 3

Course Objectives:

1. To Introduce block chain technology and Cryptocurrency.

Course Outcomes:

1. Learn about research advances related to one of the most popular technological areas today.
2. Understand Extensibility of Blockchain concepts.
3. Understand and Analyze Blockchain Science.
4. Understand Technical challenges, Business model challenges.

Unit I:

Blockchain Technology: Introduction, evolution, cryptographic primitives, elements, and significance. Cryptocurrency.

Unit II:

Consensus Protocols: The consensus problem- Byzantine Generals problem, Asynchronous Byzantine Agreement, Permissionless Models, Permissioned Models.

Unit III:

Introduction to Solidity, Smart Contracts: Ethereum, Hyperledger Fabric. Attacks on smart contracts.

Unit IV:

Decentralized Identity Management: Hyperledger Indy. Blockchain Interoperability: Hyperledger Aries. Blockchain Security.

Unit V:

Blockchain Applications: Healthcare, Preventing Cyber Crime, Tax Payments, e-voting.

Textbook:

1. Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more, 3rd Edition, Imran Bashir, Packt Publishing, 2020.
2. Arvind Narayanan, "Bitcoin and Cryptocurrency Technologies- A Comprehensive Introduction", Princeton University Press, 2016.

References:

1. Hyperledger Tutorials - https://www.hyperledger.org/use/tutorials
2. Ethereum Development Resources - https://ethereum.org/en/developers

AUTHENTICATION TECHNIQUES

B.Tech. IV Year II Sem. **L T P C**
3 - - 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 - I:
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 - II:
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 device and IoT device-based authentication; single sign- on; Symmetric Key Generation, Key Establishment, Key Agreement Protocols;

UNIT - III:
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 - IV:
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, OAuth and API.

UNIT - V:
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.

REFERENCE BOOKS:

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