



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

III Year II Semester	CYBER SECURITY & DIGITAL FORENSICS	L	T	P	C
		3	0	0	3

Course Objectives:

The aim of the course is to

- Identify security risks and take preventive steps
- understand the forensics fundamentals
- understand the evidence capturing process
- understand the preservation of digital evidence

UNIT I: Introduction to Cybercrime: Introduction, Cybercrime: Definition and Origins of the Word, Cybercrime and Information Security, Cybercriminals, Classifications of Cybercrime, Cyberstalking, Cybercafe and Cybercrimes, Botnets. Attack Vector, Proliferation of Mobile and Wireless Devices, Security Challenges Posed by Mobile Devices, Attacks on Mobile/Cell Phones, Network and Computer Attacks.

UNIT II: Tools and Methods :Proxy Servers and Anonymizers, Phishing, Password Cracking, Keyloggers and Spywares, Virus and Worms, Trojan Horses and Backdoors, Steganography, Sniffers, Spoofing, Session Hijacking Buffer over flow, DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks, Identity Theft (ID Theft), Foot Printing and Social Engineering, Port Scanning, Enumeration.

UNIT III: Cyber Crime Investigation: Introduction, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-MailRecovery, Hands on Case Studies. Encryption and Decryption Methods, Search and Seizure of Computers, Recovering Deleted Evidences, Password Cracking.

UNIT IV: Computer Forensics and Investigations: Understanding Computer Forensics, Preparing for Computer Investigations. Current Computer Forensics Tools: Evaluating Computer Forensics Tools, Computer Forensics Software Tools, Computer Forensics Hardware Tools, Validating andTesting Forensics Software, Face,Iris and Finger print Recognition, Audio Video Analysis, Windows System Forensics, Linux System Forensics, Graphics and Network Forensics, E-mail Investigations, Cell Phone and Mobile Device Forensics.

UNIT V: Cyber Crime Legal Perspectives: Introduction, Cybercrime and the Legal Landscape around the World, The Indian IT Act, Challenge to Indian Law and Cyber crime Scenario in India, Consequences of Not Addressing the Weakness in Information Technology Act, Digital Signatures and the Indian IT Act, Amendments to the Indian IT Act, Cyber crime and Punishment, Cyber law,Technology and Students:Indian Scenario.



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

Text Books:

1. Sunit Belapure Nina Godbole “Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives”, WILEY, 2011.
2. Nelson Phillips and Enfinger Steuart, “Computer Forensics and Investigations”, Cengage Learning, New Delhi, 2009.

Reference Books:

1. Michael T. Simpson, Kent Backman and James E. Corley, “Hands on Ethical Hacking and Network Defence”, Cengage, 2019.
2. Computer Forensics, Computer Crime Investigation by John R. Vacca, Firewall Media, New Delhi.
3. Alfred Basta, Nadine Basta, Mary Brown and Ravinder Kumar “Cyber Security and Cyber Laws”, Cengage, 2018.

E-Resources:

1. CERT-In Guidelines- <http://www.cert-in.org.in/>
2. <https://www.coursera.org/learn/introduction-cybersecurity-cyber-attacks> [Online Course]
3. <https://computersecurity.stanford.edu/free-online-videos> [Free Online Videos]
4. Nickolai Zeldovich. 6.858 Computer Systems Security. Fall 2014. Massachusetts Institute of Technology: MIT OpenCourseWare, <https://ocw.mit.edu> License:CreativeCommonsBY-NC-SA.



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA
KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

III Year II Semester	BLOCKCHAIN TECHNOLOGY	L	T	P	C
		3	0	0	3

Course Objectives:

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

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, 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.



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

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 Hyperledger Fabric Network, Chain codes from Developer.ibm.com, Blockchain Application Using Fabric Java SDK.

Text book:

1. “Block chain Technology”, Chandramouli Subramanian, Asha A.George, Abhilash K A and Meena Karthikeyan , Universities Press.

Reference Books:

1. Blockchain Blue print for Economy, Melanie Swan, SPD Oreilly.
2. Blockchain for Business, Jai Singh Arun, Jerry Cuomo, Nitin Gauar, Pearson Addition Wesley



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

III Year II Semester	MACHINE LEARNING	L	T	P	C
		3	0	0	3

Course Objectives:

The objectives of the course is to

- Define machine learning and its different types (supervised and unsupervised) and understand their applications.
- Apply supervised learning algorithms including decision trees and k-nearest neighbours (k-NN).
- Implement unsupervised learning techniques, such as K-means clustering.

Course Outcomes: At the end of the course, student will be able to

- Enumerate the Fundamentals of Machine Learning
- Build Nearest neighbour based models
- Apply Models based on decision trees and Bayes rule
- Make use of Linear discriminants for machine Learning
- Choose appropriate clustering technique

UNIT-I: Introduction to Machine Learning: Evolution of Machine Learning, Paradigms for ML, Learning by Rote, Learning by Induction, Reinforcement Learning, Types of Data, Matching, Stages in Machine Learning, Data Acquisition, Feature Engineering, Data Representation, Model Selection, Model Learning, Model Evaluation, Model Prediction, Search and Learning, Data Sets.

UNIT-II: Nearest Neighbor-Based Models: Introduction to Proximity Measures, Distance Measures, Non-Metric Similarity Functions, Proximity Between Binary Patterns, Different Classification Algorithms Based on the Distance Measures ,K-Nearest Neighbor Classifier, Radius Distance Nearest Neighbor Algorithm, KNN Regression, Performance of Classifiers, Performance of Regression Algorithms.

UNIT-III: Models Based on Decision Trees: Decision Trees for Classification, Impurity Measures, Properties, Regression Based on Decision Trees, Bias–Variance Trade-off, Random Forests for Classification and Regression.

The Bayes Classifier: Introduction to the Bayes Classifier, Bayes' Rule and Inference, The Bayes Classifier and its Optimality, Multi-Class Classification | Class Conditional Independence and Naive Bayes Classifier (NBC)

UNIT-IV: Linear Discriminants for Machine Learning: Introduction to Linear Discriminants, Linear Discriminants for Classification, Perceptron Classifier, Perceptron Learning Algorithm, Support Vector Machines, Linearly Non-Separable Case, Non-linear SVM, Kernel Trick, Logistic Regression, Linear Regression, Multi-Layer Perceptrons (MLPs), Backpropagation for Training an MLP.



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

UNIT-V: Clustering : Introduction to Clustering, Partitioning of Data, Matrix Factorization | Clustering of Patterns, Divisive Clustering, Agglomerative Clustering, Partitional Clustering, K-Means Clustering, Soft Partitioning, Soft Clustering, Fuzzy C-Means Clustering, Rough Clustering, Rough K-Means Clustering Algorithm, Expectation Maximization-Based Clustering, Spectral Clustering.

Text Books:

- 1.“Machine Learning Theory and Practice”, M N Murthy, V S Ananthanarayana, Universities Press (India), 2024

Reference Books:

- 1.“Machine Learning”, Tom M. Mitchell, McGraw-Hill Publication, 2017
- 2.“Machine Learning in Action”, Peter Harrington, DreamTech
- 3.“Introduction to Data Mining”, Pang-Ning Tan, Michel Stenbach, Vipin Kumar, 7th Edition, 2019.



R23 B.Tech Cyber Security
(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

III Year II Semester	SOFTWARE VULNERABILITY ANALYSIS	L	T	P	C
		3	0	0	3

Course Objectives:

- This course provides the user to know the software vulnerabilities in the real software world.
- Different application-level security
- Able to find the malicious code actions and different protection techniques.

Course Outcomes: At the end of the course, student will be able to

	Course Outcomes	Knowledge Level (K) #
CO1	Acquire the basic concepts of security & Authentication	K3
CO2	How to detect Malicious Code in software applications	K1
CO3	Analyze and apply Access Control & Physical Protection to the UNIX and Windows operating system	K4
CO4	Brief explain the concepts of OSI Model, Sockets	K2
CO5	Ability to Acquire the concepts of Counter Measures	K1

UNIT-I:

Introduction to security & Authentication- Software Security Dealing with Widespread Security Failures, Bugtraq, CERT Advisories, RISKS Digest, Technical Trends Affecting Software Security, The ileitis, Beyond Reliability, Penetrate and Patch, On Art and Engineering, Security Goals, Prevention, Traceability and Auditing, Monitoring, Privacy and Confidentiality, Multilevel Security.

UNIT-II:

Security & Malicious Code- Managing Software Security Risk: An Overview Of Software Risk Management For Security, The Role Of Security Personnel, Software Security Personnel In The Life Cycle, Deriving Requirements, Risk Assessment, Software Risk Management, Architectural Risk Analysis, Risk-Based Security Testing, Security Requirements, Security Operations.

UNIT-III:

Access Control & Physical Protection- The UNIX Access Control Model, How UNIX and Windows Exploits, Modifying File Attributes, Modifying Ownership, The unmask, The Programmatic Interface, Setuid Programming, Access Control In Windows NT, Compartmentalization, Fine-Grained Privileges. Buffer Overflow & Root kits: Buffer Overflows As Security Problems, Defending Against Buffer Overflow.



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

UNIT-IV:

Network Security& Intrusion- OSI Model, Sockets-Functions, Addresses, Network Byte Order, Internet Address Conversion, Simple Server and Web Clients, Tiny web Server. Peeling Back the Lower Layers, Network Sniffing, Raw Socket Sniffer, libpcap Sniffer, Decoding the Layers, Active Sniffing, Denial of Service, SYN Flooding, The Ping of Death, Teardrop, Ping Flooding, Amplification Attacks, Distributed DoS Flooding.

UNIT-V:

Counter Measures- Detection of System Daemons, Crash Course in Signals, Tiny web Daemon, Tools of the Trade, tiny web Exploit Tool, Log Files, Log less Exploitation, Socket Reuse, Payload Smuggling, String Encoding, Buffer Restrictions, Polymorphic Printable ASCII Shell code. Hardening Countermeasures, Non executable Stack, ret2libc, Returning into system() Randomized Stack Space, Investigations with BASH and GDB, Bouncing Off Linux gate, Applied Knowledge, First Attempts, Paying the Odds.

Text Books:

1. John Viega & Gary McGraw: Building Secure Software: How to Avoid Security Problems the Right Way (Addison-Wesley Professional Computing Series), 2001.
2. Gary McGraw: Software Security: Building Security In (Addison-Wesley Professional Computing Series), 2008.

Reference Books:

1. Michael Howard, David LeBlanc, John Viega: 19 Deadly Sins of Software Security: Programming Flaws and How to Fix Them (Security One-off) (Addison-Wesley Professional Computing Series), 2001.
2. Jon Erickson: Hacking: The Art of Exploitation, 2nd Edition (No Starch Press, San Fransico), 2005.
3. Richard Sinn “Software Security, Theory Programming and Practice” Cengage Learning, 2004.



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

III Year II Semester	DevOps	L	T	P	C
		3	0	0	3

Course Objectives:

The main objectives of this course are to:

- Describe the agile relationship between development and IT operations.
- Understand the skill sets and high-functioning teams involved in DevOps and related methods to reach a continuous delivery capability.
- Implement automated system update and DevOps lifecycle.

UNIT-I

Introduction to DevOps: Introduction to SDLC, Agile Model. Introduction to DevOps. DevOps Features, DevOps Architecture, DevOps Lifecycle, Understanding Workflow and principles, Introduction to DevOps tools, Build Automation, Delivery Automation, Understanding Code Quality, Automation of CI/ CD. Release management, Scrum, Kanban, delivery pipeline, bottlenecks, examples

UNIT-II

Source Code Management (GIT): The need for source code control, The history of source code management, Roles and code, source code management system and migrations. What is Version Control and GIT, GIT Installation, GIT features, GIT workflow, working with remote repository, GIT commands, GIT branching, GIT staging and collaboration. **UNIT TESTING - CODE COVERAGE:** Junit, nUnit& Code Coverage with Sonar Qube, SonarQube - Code Quality Analysis.

UNIT-III

Build Automation - Continuous Integration (CI): Build Automation, What is CI Why CI is Required, CI tools, Introduction to Jenkins (With Architecture), jenkins workflow, jenkins master slave architecture, Jenkins Pipelines, PIPELINE BASICS - Jenkins Master, Node, Agent, and Executor Freestyle Projects & Pipelines, Jenkins for Continuous Integration, Create and Manage Builds, User Management in Jenkins Schedule Builds, Launch Builds on Slave Nodes.



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

UNIT-IV

Continuous Delivery (CD): Importance of Continuous Delivery, CONTINUOUS DEPLOYMENT CD Flow, Containerization with Docker: Introduction to Docker, Docker installation, Docker commands, Images & Containers, DockerFile, Running containers, Working with containers and publish to Docker Hub.

Testing Tools: Introduction to Selenium and its features, JavaScript testing.

UNIT-V

Configuration Management - ANSIBLE: Introduction to Ansible, Ansible tasks, Roles, Jinjatemplating, Vaults, Deployments using Ansible.

CONTAINERIZATION USING KUBERNETES(OPENSHIFT): Introduction to Kubernetes Namespace & Resources, CI/CD - On OCP, BC, DC &ConfigMaps, Deploying Apps on Openshift Container Pods. Introduction to Puppet master and Chef.

Text Books:

1. Joyner, Joseph., Devops for Beginners: Devops Software Development Method Guide for Software Developers and It Professionals, 1st Edition MihailsKonoplows, 2015.
2. Alisson Machado de Menezes., Hands-on DevOps with Linux, 1st Edition, BPB Publications, India, 2021.

Reference Books:

1. Len Bass, Ingo Weber, Liming Zhu. DevOps: A Software Architect's Perspective. Addison Wesley; ISBN-10
2. Gene Kim Je Humble, Patrick Debois, John Willis. The DevOps Handbook, 1st Edition, IT Revolution Press, 2016.
3. Verona, Joakim Practical DevOps, 1stEdition, Packt Publishing, 2016.
4. Joakim Verona. Practical Devops, Ingram short title; 2ndedition (2018). ISBN10: 1788392574
5. Deepak Gaikwad, Viral Thakkar. DevOps Tools from Practitioner's Viewpoint. Wiley publications. ISBN: 9788126579952



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

III Year II Semester	APPLIED CRYPTOGRAPHY	L	T	P	C
		3	0	0	3

Course Objectives:

Knowledge on significance of cryptographic protocols and symmetric and public key algorithms

Course Outcomes:

1. Understand the various cryptographic protocols
2. Analyze key length and algorithm types and modes
3. Illustrate different public key algorithms in cryptosystems
4. Understand special algorithms for protocols and usage in the real world.

UNIT - I

Foundations: Terminology, Steganography, Substitution Ciphers and Transposition Ciphers, Simple XOR, One-Time Pads, Computer Algorithms, Large Numbers, Cryptographic Protocols: Protocol Building Blocks: Introduction to Protocols, Communications Using Symmetric Cryptography, One-Way Functions, One-Way Hash Functions, Communications Using Public-Key Cryptography, Digital Signatures, Digital Signatures with Encryption, Random and Pseudo-Random-Sequence Generation

UNIT - II

Cryptographic Techniques: Key length: Symmetric Key length, Public key length, comparing symmetric and public key length. Algorithm types and modes: Electronic Codebook Mode, Block Replay, Cipher Block Chaining Mode, Stream Cipher, Self-Synchronizing Stream Ciphers, Cipher-Feedback Mode, Synchronous Stream Ciphers, Output-Feedback Mod, Counter Mode, Other Block-Cipher Modes.

UNIT - III

Public-Key Algorithms: Background, Knapsack Algorithms, RSA, Pohlig-Hellman, Rabin, ElGamal, McEliece, Elliptic Curve Cryptosystems, LUC, Finite Automaton Public-Key Cryptosystems Public-Key Digital Signature Algorithms: Digital Signature Algorithm (DSA), DSA Variants, Gost Digital Signature Algorithm, Discrete Logarithm Signature Schemes, Ong-Schnorr-Shamir, ESIGN



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

UNIT - IV

Special Algorithms for Protocols: Multiple-Key Public-Key Cryptography, Secret-Sharing Algorithms, Subliminal Channel, Undeniable Digital Signatures, Designated Confirmer Signatures, Computing with Encrypted Data, Fair Coin Flips, One-Way Accumulators, All-or-Nothing Disclosure of Secrets, Fair and Failsafe Cryptosystems, Zero-Knowledge Proofs of Knowledge, Blind Signatures, Oblivious Transfer, Secure Multiparty Computation, Probabilistic Encryption, Quantum Cryptography

UNIT - V

Real World Approaches: IBM Secret key management protocol, ISDN, Kerberos, KryptoKnight, Privacy enhanced mail (PEM), Message security protocol (MSP), PGP, Public-Key Cryptography Standards (PKCS), Universal Electronic Payment System (UEPS).

Text books:

1. Bruce Schneier, Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C (cloth)



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA
KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security
(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

III Year II Semester	INTERNET OF THINGS	L	T	P	C
		3	0	0	3

Course Objectives:

From the course the student will learn

- the application areas of IOT
- the revolution of Internet in Mobile Devices, Cloud & Sensor Networks
- building blocks of Internet of Things and characteristics

UNIT I:

Predecessors of IoT: Introduction, Wireless Sensor Networks, Machine-to-Machine Communications, Cyber Physical Systems. Emergence of IoT: Introduction, Evolution of IoT, Enabling IoT and the Complex Interdependence of Technologies, IoT Networking Components, Addressing Strategies in IoT

UNIT II:

IoT Sensing and Actuation: Introduction, Sensors, Sensor Characteristics, Sensorial Deviations, Sensing Types, Sensing Considerations, Actuators, Actuator Types, Actuator Characteristics. IoT Processing Topologies and Types: Data Format, Importance of Processing in IoT, Processing Topologies, IoT Device Design and Selection Considerations, Processing Offloading.

UNIT III:

IoT Connectivity Technologies: Introduction, IEEE 802.15.4, Zigbee, Thread, ISA100.11A, WirelessHART, RFID, NFC,DASH7, Z-Wave, Weightless, Sigfox, LoRa, NB-IoT, Wi-Fi, Bluetooth. IoT Communication Technologies: Introduction, Infrastructure Protocols, Discovery Protocols, Data Protocols, Identification Protocols, Device Management, Semantic Protocols.

UNIT IV:

IoT Interoperability: Introduction, Standards, Frameworks. Fog Computing and Its Applications: Introduction, View of Fog Computing Architecture, Fog Computing in IoT, Selected Applications of Fog Computing

UNIT V:

Paradigms, Challenges, and the Future: Introduction, Evolution of New IoT Paradigms, Challenges Associated with IoT, Emerging Pillars of IoT. IoT Case Studies: Agricultural IoT, Vehicular IoT



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

Text Books:

1. Introduction to IoT, Sudip Misra, Anandarup Mukherjee, Arjit Roy, Cambridge University Press, 2021
2. Internet of Things: Architecture, Design Principles and Applications, Rajkamal, McGraw Hill Higher Education

Reference Books:

1. Fog and Edge Computing: Principles and Paradigms, [Rajkumar Buyya \(Editor\)](#), [Satish Narayana Srirama \(Editor\)](#), ISBN: 978-1-119-52498-4, January 2019
2. Getting Started with the Internet of Things, Cuno Pfister, O'Reilly



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

III Year II Semester	DESIGN OF SECURE PROTOCOLS	L	T	P	C
		3	0	0	3

Course objectives:

The main objective of this course is that to explore various protocols and design of various protocols with deeper security.

Course Outcomes:

- Get the exposure to various protocols.
- Gain knowledge on various secure mechanisms through set of protocols.
- Apply different data link layer protocols
- Efficiently design new set of protocols.
- Learn Security issues and over come means with protocols.

UNIT-I

OSI: ISO Layer Protocols:- Application Layer Protocols-TCP/IP, HTTP, SHTTP, LDAP, MIME, - POP & POP3 - RMON-SNTP-SNMP. Presentation Layer Protocols –Light Weight Presentation Protocol Session layer protocols.

UNIT-II

RPC protocols transport layer protocols ITOT,RDP,RUDP,TALI,TCP/UDP, compressed TCP. Network layer Protocols – routing protocols-border gateway protocol-exterior gateway protocol-internet protocol IPv4- IPv6- Internet Message Control Protocol- IRDP- Transport Layer Security-TSL-SSL-DTLS

UNIT-III

Data Link layer Protocol – ARP – In ARP – IPCP – IPv6CP – RARP – SLIP .Wide Area and NetworkProtocols- ATM protocols – Broadband Protocols – Point to Point Protocols – Other WAN Protocols-security issues.

UNIT-IV

Local Area Network and LAN Protocols – ETHERNET Protocols–VLAN protocols–Wireless LAN Protocols–Metropolitan Area Network Protocol–Storage Area Network and SAN



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

UNIT-V

Protocols - FDMA, WIFI and WIMAX Protocols - security issues. Mobile IP – Mobile Support Protocol for IPv4 and IPv6 – Resource Reservation Protocol. Multi – casting Protocol–VGMP, IGMPMSDP. Network Security and Technologies and Protocols–AAA Protocols–Tunneling Protocols– Secured Routing Protocols– GRE-Generic Routing Encapsulation– IPSEC–Security.

TEXTBOOKS:

1. Jawin: "Networks Protocols Handbook", 3rd Edition, Jawin Technologies Inc., 2005.
2. Bruce Potter and Bob Fleck: "802.11 Security", 1st Edition, O'Reilly Publications, 2002.

REFERENCES:

1. Ralph Oppiger: "SSL and TLS: Theory and Practice", 1st Edition, Artech House, 2009.
2. Lawrence Harte: "Introduction to CDMA-Network services Technologies and Operations", 1st Edition , Althos Publishing, 2004.
3. Lawrence Harte: "Introduction to WIMAX", 1st Edition, Althos Publishing, 2005.



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

III Year II Semester	FIREWALLS & VPN SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

- Identify and assess current and anticipated security risks and vulnerabilities
- Develop a network security plan and policies
- Establish a VPN to allow IPSec remote access traffic
- Monitor, evaluate and test security conditions and environment
- Develop critical situation contingency plans and disaster recovery plan
- Implement/test contingency and backup plans and coordinate with stakeholders
- Monitor, report and resolve security problems

Course Outcomes: At the end of the course, student will be able to

- To show the fundamental knowledge of Firewalls and its types
- Construct a VPN to allow Remote Access, Hashing, connections with Cryptography and VPN Authorization
- Elaborate the knowledge of depths of Firewalls, Interpreting firewall logs, alerts, Intrusion and Detection
- Infer the design of Control Systems of SCAD, DCS, PLC's and ICS's
- Evaluate the SCADA protocols like RTU, TCP/IP, DNP3, OPC, DA/HAD

SYLLABUS

UNIT-I: Firewall Fundamentals-Introduction, Types of Firewalls, Ingress and Egress Filtering, Types of Filtering, Network Address Translation (NAT), Application Proxy, Circuit Proxy, Content Filtering, Software versus Hardware Firewalls, IPv4 versus IPv6 Firewalls, Dual-Homed and Triple-Homed Firewalls, Placement of Firewalls.

UNIT-II: VPN Fundamentals-VPN Deployment Models and Architecture, Edge Router, Corporate Firewall, VPN Appliance, Remote Access, Site-to-Site, Host-to-Host, Extranet Access, Tunnel versus Transport Mode, The Relationship Between Encryption and VPNs, Establishing VPN Connections with Cryptography, VPN Authorization.

UNIT-III: Exploring the Depths of Firewalls-Firewall Rules, Authentication and Authorization, Monitoring and Logging, Understanding and Interpreting Firewall Logs and Alerts, Intrusion Detection, Limitations of Firewalls, Downside of Encryption with Firewalls, Firewall Enhancements and Management Interfaces.



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

UNIT–IV: Overview of Industrial Control Systems-Overview of SCADA, DCS, and PLCs, ICS Operation, Key ICS Components, Control Components, Network Components, SCADA Systems, Distributed Control Systems, Programmable Logic Controllers, Industrial Sectors and their Interdependencies.

UNIT–V: SCADA Protocols-Modbus RTU, Modbus TCP/IP, DNP3, DNP3 TCP/IP, OPC, DA/HAD, SCADA protocol fuzzing. Finding Vulnerabilities in HMI: software- Buffer Overflows, Shell code. Previous attacks Analysis- Stuxnet, Duqu.

Text Books:

1. Michael Stewart “Network Security, Firewalls, and VPNs” Jones & Bartlett Learning September 2010.
2. T. Macaulay and B. L. Singer, Cyber security for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS, Auerbach Publications, 2011.

Reference Books:

1. J. Lopez, R. Setola, and S. Wolthusen, Critical Infrastructure Protection Information Infrastructure Models, Analysis, and Defense, Springer-Verlag Berlin Heidelberg, 2012.
2. Robert Radvanovsky and Jacob Brodsky, editors. Handbook of SCADA/Control Systems Security. CRC Press, 2013.
3. A.W. Colombo, T. Bangemann, S. Karnouskos, S. Delsing, P. Stluka, R. Harrison, et al. Industrial cloud-based cyber-physical systems Springer International Publishing, 2014.
4. D. Bailey, Practical SCADA for Industry. Burlington, MA: Newnes, 2003.



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA
KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security
(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

III Year II Semester	WEB APPLICATION SECURITY	L	T	P	C
		3	0	0	3

Prerequisites: Networking Fundamentals, Web Development Basics and Cyber security Fundamentals

Course Objectives: This course aims to provide students with a fundamental understanding of web application security principles, common vulnerabilities, and security best practices.

Course Outcomes:

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

CO1- Identify and analyze web application security vulnerabilities.

CO2- Apply secure coding practices to develop and maintain web applications.

CO3- Perform security testing and assessment on web applications.

CO4- Configure and manage Web Application Firewalls (WAFs) for protection.

CO5- Develop an incident response plan for web application security breaches.

UNIT I: **(9 Hours)**

Introduction to Web Application Security: Introduction to web application security concepts, Importance of web application security, Threat landscape and security challenges in web applications, The role of security in the software development lifecycle

UNIT II: **(9 Hours)**

Web Application Vulnerabilities: Common web application vulnerabilities (e.g., SQL injection, XSS, CSRF), Understanding attack vectors and exploitation techniques, Real-world examples of web application breaches and their impact, Introduction to the OWASP Top Ten Project

UNIT III: **(10 Hours)**

Secure Coding Practices: Principles of secure coding for web applications, Input validation and sanitization, Authentication and authorization mechanisms, Session management and secure communication, Error handling and logging

UNIT IV: **(9 Hours)**

Web Application Security Testing: Manual and automated security testing techniques, Vulnerability scanning and assessment tools, Security testing methodologies (e.g., black-box, white-box, gray-box testing), Reporting and remediation of security findings



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

UNIT V:

(9 Hours)

Web Application Firewall (WAF) and Incident Response: Introduction to Web Application Firewalls (WAF), Deploying and configuring WAF for web application protection, Incident response and handling security breaches, Web application security monitoring and alerting.

TEXT BOOKS:

1. "Web Application Security: A Beginner's Guide" by Bryan Sullivan, Vincent Liu
2. "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" by DafyddStuttard and Marcus Pinto
3. "Secure Coding in C and C++" by Robert C. Seacord (For secure coding practices)
4. "OWASP Testing Guide" by The OWASP Foundation (Free online resource for security testing)

REFERENCE BOOKS:

1. "Web Application Security: Threats, Countermeasures, and Best Practices" by Lakshmanan Ganapathy and Mike Ware
2. "Hacking Web Apps: Detecting and Preventing Web Application Security Problems" by Mike Shema
3. "Secure Programming with Static Analysis" by Brian Chess and Jacob West



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA
KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security
(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

III Year II Semester	SECURITY ASSESSMENT AND RISK ANALYSIS	L	T	P	C
		3	0	0	3

COURSE OBJECTIVES

1. The course takes a software development perspective to the challenges of engineering software systems that are secure.
2. This course addresses design and implementation issues critical to producing secure software systems.
3. The course deals with the question of how to make the requirements for confidentiality, integrity, and availability integral to the software development process.
4. Secure software requirements gathering to design, development, configuration, deployment, and ongoing maintenance
5. Security of enterprise information systems.

COURSE OUTCOMES:

1. Understand various aspects and principles of software security.
2. Devise security models for implementing at the design level.
3. Identify and analyze the risks associated with s/w engineering and use relevant models to mitigate the risks.
4. Understand the various security algorithms to implement for secured computing and computer networks
5. Explain different security frameworks for different types of systems including electronic systems.

UNIT-I

Defining computer security, the principles of secure software, trusted computing base, etc, threat modeling, advanced techniques for mapping security requirements into design specifications. Secure software implementation, deployment and ongoing management.

UNIT-II

Software design and an introduction to hierarchical design representations.Difference between high-level and detailed design.Handling security with high-level design. General Design Notions. Security concerns designs at multiple levels of abstraction, Design patterns, quality assurance activities and strategies that support early vulnerability detection, Trust models, security Architecture & design reviews .



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

UNIT-III

Software Assurance Model: Identify project security risks & selecting risk management strategies, Risk Management Framework, Security Best practices/ Known Security Flaws, Architectural risk analysis, Security Testing & Reliability (Penn testing, Risk- Based Security Testing

UNIT-IV

Security in Enterprise Business: Identification and authentication, Enterprise Information Security, Symmetric and asymmetric cryptography, including public key cryptography, data encryption standard (DES), advanced encryption standard (AES), algorithms for hashes and message digests. Authentication, authentication schemes , access control models, Kerberos protocol, public key infrastructure (PKI), protocols specially designed for e-commerce and web applications, firewalls and VPNs.

UNIT-V

Security development frameworks. Security issues associated with the development and deployment of information systems, including Internet-based e-commerce, e-business, and e-service systems.

TEXT BOOKS:

1. W. Stallings, Cryptography and network security: Principles and practice, 5 th Edition, Upper Saddle River, NJ: Prentice Hall., 2011
2. C. Kaufman, r. Perlman, & M. Speciner, Network security: Private communication in a public world, 2 nd Edition, Upper Saddle River, NJ:PrenticeHall, 2002
3. C. P. Pfleeger, S. L. Pfleeger, Security in Computing, 4 th Edition, Upper Saddle River, NJ:Prentice Hall, 2007
4. T. M. Merkow, & J. Breithaupt, Information security: Principles and practices. Upper Saddle River, NJ:Prentice Hall, 2005

REFERENCE BOOKS:

1. Gary McGraw, Software Security: Building Security In, Addison-Wesley, 2006



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA
KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security
(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

III Year II Semester	CYBER SECURITY & DIGITAL FORENSICS LAB	L	T	P	C
		0	0	3	1.5

Course Objectives:

- Investigate cybercrime and collect evidences
- Able to use knowledge of forensic tools and software
- To understand the preservation of digital evidence.
- To learn about stenography Perceptual models

Course Outcomes: At the end of the course, student will be able to

	Course Outcomes	Knowledge Level (K) #
CO1	Identify the importance of a systematic procedure for investigation of data found on digital storage media that might provide evidence of wrong-doing.	K3
CO2	Construct the file system storage mechanisms of two common desktop operating systems and forensics tools used in data analysis.	K6
CO3	List and Implement all running processes, network connections from a memory image and find whether a firewall is set by analyzing a memory image.	K4
CO4	Define and perform live incident response on a system, View all browser history and List out all established network connections in a computer (Hint: Triage Incident Response).	K1

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												
CO4												

(Please fill the above with Levels of Correlation, viz., L, M, H)



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

Experiment- 1

Evidence Collection

- a) Linux: Capturing RAM dump using fmem

<https://github.com/NateBrune/fmem>

i) dcfldd if=/dev/fmem of=memory.dump hash=sha256
sha256log=memory.dump.sha256 bs=1MB count=1000

- b) Linux: Capturing Disk using dfldd

<https://www.obsidianforensics.com/blog/imaging-using-dcfldd>

i) dcfldd if=/dev/sdb1 of=/media/disk/test_image.dd hash=md5,
sha1hashlog=/media/disk/hashlog.txt

- c) Windows: Capture RAM dump of a windows system

a. Hint: FTK Imager or RAMCapture

- d) Windows: Capture Disk Image of a windows system

Hint: FTK Imager

Experiment- 2

Disk Analysis

- i) List all files in a directory from a disk image
 - a. FTK Imager
- ii) Export a particular file from a disk image
 - a. FTK Imager
- iii) Recover a deleted file from a disk image

FTK Imager

Experiment- 3

Memory Analysis

1. List all running processes from a memory image
2. List all network connections from a memory image
3. Find out whether a firewall is set by analyzing a memory image

Hint: volatility

Experiment- 4

- 4) Live Incident Response

1. Perform live incident response on a system
2. View all browser history in a computer
3. List out all established network connections in a computer

Hint: Triage Incident Response



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

Exercise- 5

Implement E-Mail Tracking and Email Investigation

Exercise- 6

Implement video Analytics for a live video

Exercise- 7

Analysis on different Malware Working

Exercise- 8

Work on Mail Bombs &SMS bombs

Exercise- 9

Implement a case on windows and Linux forensics

Exercise- 10

Implement a case on network Forensic

Exercise- 11

Work on different types of vulnerabilities

Exercise- 12

Implement a case on Mobile Forensics

Exercise- 13

Develop a Evidence and Preparation and Documentation



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

III Year II Semester	MALWARE ANALYSIS & REVERSE ENGINEERING LAB	L	T	P	C
		0	0	3	1.5

COURSE OBJECTIVES:

- This course provides students a foundational knowledge about reverse engineering and malware analysis, through the study of various cases.
- This course provides students a hand-on analysis of malware samples.
- It covers fundamental concepts in malware investigations so as to equip the students with enough background knowledge in handling malicious software attacks.

COURSE OUTCOMES:

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

- CO 1:** Demonstrate the cyber security challenges posed by malicious software attacks. [K2]
CO 2: Analyze security risks, threats and potential vulnerabilities in enterprise networks environment. [K3]
CO 3: Independently to conduct in-depth analysis of modern malware samples using behavioural, code analysis and memory forensic techniques. [K3]
CO 4: Apply the techniques learned to proactively protect computer systems and networks, reduce security risks and mitigate the potential for malicious software attacks. [K5]
CO 5: Apply immunity debugger for reverse engineering [K3]

EXPERIMENTS:

WEEK-1: Malware analysis lab environment setup

WEEK-2: Building malwares using tools

WEEK-3: Static Malware Analysis

1. Upload the files to <http://www.VirusTotal.com/> and view the reports. Does either file match any existing antivirus signatures?
2. When were these files compiled?
3. Are there any indications that either of these files is packed or obfuscated? If so, what are these indicators?
4. Do any imports hint at what this malware does? If so, which imports are they?
5. Are there any other files or host-based indicators that you could look for on infected systems?
6. What network-based indicators could be used to find this malware on infected machines?
7. What would you guess is the purpose of these files?



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

WEEK-4: Static Malware Analysis

1. Upload the Lab01-02.exe file to <http://www.VirusTotal.com/>. Does it match any existing antivirus definitions?
2. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.
3. Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?
4. What host- or network-based indicators could be used to identify this malware on infected machines

WEEK-5: Dynamic Malware Analysis

1. How can you get this malware to install itself?
2. What are the command-line options for this program? What is the password requirement?
3. How can you use OllyDbg to permanently patch this malware, so that it doesn't require the special command-line password?
4. What are the host-based indicators of this malware?
5. What are the different actions this malware can be instructed to take via the network?
6. Are there any useful network-based signatures for this malware?

WEEK-6: Dynamic Malware Analysis

1. What strings do you see statically in the binary?
2. What happens when you run this binary?
3. How can you get this sample to run its malicious payload?
4. What is happening at 0x00401133?
5. What arguments are being passed to subroutine 0x00401089?
6. What domain name does this malware use?
7. What encoding routine is being used to obfuscate the domain name?
8. What is the significance of the Create Process A call at 0x0040106E?

WEEK-7: Automated Malware Analysis

WEEK-8: Android malware analysis using tools

WEEK-9: Malware hunting Techniques using 1.Backdoors 2.Ransomware

WEEK-10: Malware hunting Techniques using 1.Credential stealers
2. Persistence mechanisms

WEEK-11: Host exploitation and forensic analysis

WEEK-12:

1. Reverse Engineering with Immunity Debugger
2. Software Cracking with HexEditor Tool
3. Rebuilding the software after cracking



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

Text Books:

1. Sikorski, M., & Honig, A. (2012). Practical malware analysis: the hands-on guide to dissecting malicious software. No starch press.
2. Eilam, E. (2005). Reversing, Secrets of Reverse Engineering Wiley Publishing.
3. Malin, C. H. (2013). Linux Malware Incident Response: A Practitioner's Guide to Forensic Collection and Examination of Volatile Data: An Excerpt from Malware Forensic FieldGuide for Linux Systems. Elsevier.

Reference Books:

1. Sikorski, M., & Honig, A. (2012). Practical malware analysis: the hands-on guide to dissecting malicious software. No starch press.
2. Shashidhar, N., & Cooper, P. (2016, April). Teaching malware analysis: The designphilosophy of a model curriculum. In 2016 4th International Symposium on Digital Forensic andSecurity (ISDFS) (pp. 119-125). IEEE.
3. Singh, A.(Ed.). (2009). Identifying malicious code through reverse engineering (Vol. 4).Springer Science & Business Media.



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

III Year II Semester	SOFT SKILLS or IELTS	L	T	P	C
		0	1	2	2

Course Objectives:

- To equip the students with the skills to effectively communicate in English
- To train the students in interview skills, group discussions and presentation skills
- To motivate the students to develop confidence
- To enhance the students' interpersonal skills
- To improve the students' writing skills

UNIT -I

Analytical Thinking & Listening Skills: Self-Introduction, Shaping Young Minds - A Talk by Azim Premji (Listening Activity), Self – Analysis, Developing Positive Attitude, Perception. Communication Skills: Verbal Communication; Non Verbal Communication (Body Language)

UNIT -II

Self-Management Skills: Anger Management, Stress Management, Time Management, Six Thinking Hats, Team Building, Leadership Qualities. Etiquette: Social Etiquette, Business Etiquette, Telephone Etiquette, Dining Etiquette

UNIT - III

Standard Operation Methods: Basic Grammars, Tenses, Prepositions, Pronunciation, Letter Writing; Note Making, Note Taking, Minutes Preparation, Email & Letter Writing

UNIT-IV

Job-Oriented Skills: Group Discussion, Mock Group Discussions, Resume Preparation, Interview Skills, Mock Interviews

UNIT-V

Interpersonal relationships: Introduction, Importance, Types, Uses, Factors affecting interpersonal relationships, Accommodating different styles, Consequences of interpersonal relationships

Text books:

1. Barun K. Mitra, Personality Development and Soft Skills, Oxford University Press, 2011.
2. S.P. Dhanavel, English and Soft Skills, Orient Blackswan, 2010.

Reference books:

1. R.S. Aggarwal, A Modern Approach to Verbal & Non-Verbal Reasoning, S.Chand & Company Ltd., 2018.
2. Raman, Meenakshi & Sharma, Sangeeta, Technical Communication Principles and Practice, Oxford University Press, 2011.

E-resources:

https://swayam-plus.swayam2.ac.in/courses/course-details?id=P_CAMBR_01



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA
KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security
(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

III Year II Semester	TECHNICAL PAPER WRITING & IPR	L	T	P	C
		2	0	0	0

Course Objective :

- The course will explain the basic related to writing the technical reports and understanding the concepts related to formatting and structuring the report.
- This will help students to comprehend the concept of proofreading, proposals and practice

UNIT-I

Introduction: An introduction to writing technical reports, technical sentences formation, using transitions to join sentences, Using tenses for technical writing. **Planning and Structuring:** Planning the report, identifying reader(s), Voice, Formatting and structuring the report, Sections of a technical report, Minutes of meeting writing.

UNIT-II

Drafting report and design issues: The use of drafts, Illustrations and graphics.**Final edits:** Grammar, spelling, readability and writing in plain English: Writing in plain English, Jargon and final layout issues, Spelling, punctuation and Grammar, Padding, Paragraphs, Ambiguity.

UNIT-III

Proofreading and summaries: Proofreading, summaries, Activities on summaries. **Presenting final reports:** Printed presentation, Verbal presentation skills, Introduction to proposals and practice.

UNIT-IV Using word processor:

Adding a Table of Contents, Updating the Table of Contents, Deleting the Table of Contents, Adding an Index, Creating an Outline, Adding Comments, Tracking Changes, Viewing Changes, Additions, and Comments, Accepting and Rejecting Changes, Working with Footnotes and Endnotes, Inserting citations and Bibliography, Comparing Documents, Combining Documents, Mark documents final and make them read only., Password protect Microsoft Word documents., Using Macros,

UNIT-V

Nature of Intellectual Property: Patents, Designs, Trade and Copyright. Process of **Patenting and Development:** technological research, innovation, patenting, development. International Scenario: International cooperation on Intellectual Property



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

Text Books:

1. Kompal Bansal & Parshit Bansal, "Fundamentals of IPR for Beginner's", 1st Ed., BS Publications, 2016.
2. William S. Pfeiffer and Kaye A. Adkins, "Technical Communication: A Practical Approach", Pearson.
3. Ramappa,T., "Intellectual Property Rights Under WTO", 2nd Ed., S Chand, 2015.

Reference Books:

1. Adrian Wallwork , English for Writing Research Papers, Springer New York Dordrecht Heidelberg London, 2011.
2. Day R, How to Write and Publish a Scientific Paper, Cambridge University Press(2006)

E-resources:

1. <https://www.udemy.com/course/reportwriting/>
2. <https://www.udemy.com/course/professional-business-english-and-technical-report-writing/>
3. <https://www.udemy.com/course/betterbusinesswriting/>



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

MINORS

	COMPUTER NETWORKS	L	T	P	C
		3	0	0	3

Course Objectives:

- To understand the different types of networks
- To discuss the software and hardware components of a network
- To develop an understanding the principles of computer networks.
- To familiarize with OSI model and the functions of layered structure.
- To explain networking protocols, algorithms and design perspectives.

Course Outcomes (CO): After completion of the course, students will be able to

- Identify the software and hardware components of a Computer network. (L1)
- Explain the functionality of each layer of a computer network. (L2)
- Identify and analyze flow control, congestion control, and routing issues. (L4)
- Analyze and interpret the functionality and effectiveness of the routing protocols. (L4)
- Choose the appropriate transport protocol based on the application requirements. (L3)

UNIT-I

Introduction: Types of Computer Networks, Broadband Access Networks, Mobile and Wireless Access Networks, Content Provider Networks, Transit networks, Enterprise Networks, Network technology from local to global, Personal Area Networks, Local Area Networks, Home Networks, Metropolitan Area Networks, Wide Area Networks, Internetworks, Network Protocols, Design Goals, Protocol Layering, Connections and Reliability, Service Primitives, The Relationship of Services to Protocols ,Reference Models, The OSI Reference Model, The TCP/IP Reference Model, A Critique of the OSI Model and Protocols, A Critique of the TCP/IP Reference Model and Protocols.

UNIT-II

The Data Link Layer: Guided Transmission Media, Persistent Storage, Twisted Pairs, Coaxial Cable, Power Lines, Fiber Optics, Data Link Layer Design Issues, Services Provided To The Network Layer, Framing Error Control, Flow Control, Error Detection And Correction, Error-Correcting Codes, Error-Detecting Codes, Elementary Data Link Protocols, Initial Simplifying Assumptions Basic Transmission And Receipt, Simplex Link-Layer Protocols, Improving Efficiency, Bidirectional Transmission, Multiple Frames In Flight, Examples Of Full-Duplex, Sliding Window Protocols, The Channel Allocation Problem, Static Channel Allocation, Assumptions For Dynamic Channel Allocation, Multiple Access Protocols, Aloha, Carrier Sense Multiple Access Protocols, Collision-Free Protocols, Limited-Contention Protocols, Wireless LAN Protocols, Ethernet, Classic Ethernet Physical Layer, Classic Ethernet Mac Sublayer Protocol, Ethernet Performance, Switched Ethernet,



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet, 40- And 100-Gigabit Ethernet, Retrospective On Ethernet.

UNIT-III

The Network Layer: Network Layer Design Issues, Store-And-Forward Packet Switching, Services Provided To The Transport Layer, Implementation Of Connectionless Service, Implementation Of Connection-Oriented Service, Comparison Of Virtual-Circuit And Datagram Networks, Routing Algorithms In A Single Network, The Optimality Principle, Shortest Path Algorithm, Flooding, Distance Vector Routing, Link State Routing, Hierarchical Routing Within a Network, Broadcast Routing, Multicast Routing, Anycast Routing, Traffic Management at The Network Layer, The Need for Traffic Management: Congestion, Approaches To Traffic Management, Internetworking, Internetworks: An Overview, How Networks differ, Connecting Heterogeneous Networks, Connecting Endpoints Across Heterogeneous Networks, Internetwork Routing: Routing Across Multiple Networks Supporting Different Packet Sizes: Packet Fragmentation, The Network Layer In The Internet, The IP Version 4 Protocol, IP Addresses, IP Version 6, Internet Control Protocols, Label Switching and MPLS, OSPF—An Interior Gateway Routing Protocol, BGP—The Exterior Gateway Routing Protocol, Internet Multicasting.

UNIT-IV

The Transport Layer: The Transport Service, Services Provided To The Upper Layers, Transport Service Primitives, Berkeley Sockets, An Example Of Socket Programming: An Internet File Server, Elements Of Transport Protocols, Addressing, Connection Establishment, Connection Release, Error Control And Flow Control, Multiplexing, Crash Recovery, Congestion Control, Desirable Bandwidth Allocation, Regulating The Sending Rate, Wireless Issues, The Internet Transport Protocols: UDP, Introduction To UDP, Remote Procedure Call, Real-Time Transport Protocols, The Internet Transport Protocols: TCP, Introduction To TCP, The TCP Service Model, The TCP Protocol, The TCP Segment Header, TCP Connection Establishment, TCP Connection Release.

UNIT-V

The Application Layer: Electronic Mail, Architecture and Services, The User Agent, Message Formats, Message Transfer, Final Delivery, The World Wide Web, Architectural Overview, Static Web Objects, Dynamic Web Pages and Web Applications, HTTP and HTTPS, Web Privacy, Content Delivery, Content and Internet Traffic, Server Farms and Web Proxies, Content Delivery Networks, Peer-To-Peer Networks, Evolution of The Internet.



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

Textbook:

1. Andrew Tanenbaum, Feamster Wetherall, Computer Networks, 6th Edition, Global Edition.

Reference Books:

1. Behrouz A. Forouzan, Data Communications and Networking, 5th Edition, McGraw Hill Publication, 2017.
2. James F. Kurose, Keith W. Ross, “Computer Networking: A Top-Down Approach”, 6th edition, Pearson, 2019.
3. YouluZheng, ShakilAkthar, “Networks for Computer Scientists and Engineers”, Oxford Publishers, 2016.

Online Learning Resources:

<https://nptel.ac.in/courses/106105183/25>

<http://www.nptelvideos.in/2012/11/computer-networks.html>

<https://nptel.ac.in/courses/106105183>



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

	INTRODUCTION TO CYBER SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

- Understand the threats in networks and security concepts.
- Apply authentication applications in different networks.
- Understand security services for email.
- Awareness of firewall and its applications.

Course Outcomes: By the end of the course, the student should be able to:

- Differentiate among different types of security attacks.
- Define computer forensics.
- Identify the process in taking digital evidence.
- Describe how to conduct an investigation using methods of memory, operating system, network and email forensics with different forensic tools.

UNIT-I

Introduction to Information Security Fundamentals and Best Practices: Protecting Your Computer and its Contents, Securing Computer Networks--Basics of Networking, Compromised Computers, Secure Communications and Information Security Best Practices, Privacy Guidelines, Safe Internet Usage.

UNIT-II

Ethics in Cyber Security & Cyber Law: Privacy, Intellectual Property, Professional Ethics, Freedom of Speech, Fair User and Ethical Hacking, Trademarks, Internet Fraud, Electronic Evidence, Cybercrimes.

UNIT-III

Penetration Testing: Overview of the web from a penetration tester's perspective, Exploring the various servers and clients, Discussion of the various web architectures, Discussion of the different types of vulnerabilities, defining a web application test scope and process, Defining types of penetration testing.



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

UNIT-IV

Web Application Security: Common Issues in Web Apps, what is XSS, SQL injection, CSRF, Password Vulnerabilities, SSL, CAPTCHA, Session Hijacking, Local and Remote File Inclusion, Audit Trails, Web Server Issues. **Forensics & Network Assurance:** Forensic Technologies, Digital Evidence Collection, Evidentiary Reporting, Layered Defense, Surveillance and Reconnaissance, Outsider Thread Protection

UNIT-V

Information Risk Management: Asset Evaluation and Business Impact Analysis, Risk Identification, Risk Quantification, Risk Response Development and Control, Security Policy, Compliance, and Business Continuity. Forensic investigation using Access Data FTK, En-Case

Cyber Incident Analysis and Response: Incident Preparation, Incident Detection and Analysis. Containment, Eradication, and Recovery. Proactive and Post-Incident Cyber Services, CIA triangle

Text Books:

1. Cyber Security & Digital Forensics by Anas Zakir, Clever Fox Publishing, Publication Date- 2022
2. “Beginners Guide To Ethical Hacking and Cyber Security “, by Abhinav Ojha, Khanna Publishers, First Edition, Publication Date-2023

Reference Books:

1. The Official CHFI Study Guide for Computer Hacking Forensic Investigator by Dave Kleiman
2. CISSP Study Guide, 6th Edition by James M. Stewart



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

	CRYPTOGRAPHY & NETWORK SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

- Explain the objectives of information security
- Explain the importance and application of each of confidentiality, integrity, authentication and availability
- Understand the basic categories of threats to computers and networks
- Discusses the Mathematics of Cryptography
- Discuss the fundamental ideas of Symmetric and Asymmetric cryptographic Algorithms
- Discusses the Network layer, Transport Layer and Application layer Protocols Enhanced security mechanisms

Course Outcomes: At the end of the course, student will be able to

CO	Course Outcomes	Knowledge Level (K) #
CO1	Student will be able to understand security issues related to computer networks and learn different symmetric key techniques	K2
CO2	Students will be able learn mathematic of cryptography for symmetric and Asymmetric algorithms and apply this knowledge to understand the Cryptographic algorithms	K3
CO3	Students will be able learn different types of symmetric and Asymmetric algorithms	K3
CO4	Students will be able learn different algorithms of Hash functions, message authentication and digital signature and their importance to the security	K4
CO5	Students will be able learn different Enhanced security protocols of Application Layer, Transport Layer and Network layer	K4

#Based on suggested Revised BTL



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

Mapping of course outcomes with program outcomes

	P O1	P O2	P O3	P O4	P O5	P O6	P O7	P O8	P O9	PO 10	PO 11	PO 12	PS O1	PS O2	PS O3
C O1	1	2	1	2	1	1	1	1		1		2	2	2	2
C O2	3	1	1	2	2	2	1	2		3	3	2	3	2	1
C O3	2	2	2	1	2	1	1	1		2		3	1		
C O4	3	2	3	2	3	2	1	1		2	1	2	2	1	
C O5	3	2	3	1	2	2	1	1		2	2	2	1	2	1

(Please fill the above with Levels of Correlation, viz., L-1, M-2, H-3)

UNIT-I

Security Concepts: Introduction, The need for security, Security approaches, Principles of security, Types of Security attacks, Security services, Security Mechanisms, A model for Network Security Cryptography. Classical Encryption Techniques-symmetric cipher model, Substitution techniques, Transposition techniques, Rotor Machines, Stenography.

UNIT-II

Introduction to Symmetric Cryptography: Algebraic Structures-Groups, Rings, Fields, $GF(2^n)$ fields, Polynomials. **Mathematics of Asymmetric cryptography:** Primes, Checking For Primeness, Eulers phi-functions, Fermat's Little Theorem, Euler's Theorem, Generating Primes, Primality Testing, Factorization, Chinese Remainder Theorem, Quadratic Congruence, Exponentiation And Logarithm.

UNIT-III

Symmetric key Ciphers: Block Cipher principles, DES, AES, Blowfish, IDEA, Block cipher operation, Stream ciphers: RC4, RC5. **Asymmetric key Ciphers:** Principles of public key cryptosystems, RSA algorithm, Diffie-Hellman Key Exchange, Elgamal Cryptographic system, Elliptic Curve Arithmetic, Elliptic Curve Cryptography.



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

UNIT-IV

Cryptographic Hash Functions: Applications of Cryptographic Hash Functions, Two Simple Hash Functions, Requirements and Security, Hash Functions Based on Cipher Block Chaining, Secure Hash Algorithms (SHA). **Message Authentication Codes:** Message Authentication Requirements, Message Authentication Functions, Requirements for Message Authentication Codes, Security of MAC'S, MAC'S Based on Hash Functions: HMAC, MAC'S Based On Block Ciphers: DAA And CMAC. **Digital Signatures:** Digital Signatures, Elgamal Digital Signature Scheme, Elliptic Curve Digital Signature Algorithm, RSA-PSS Digital Signature Algorithm.

UNIT-V

Network and Internet Security: **Transport-Level Security:** Web Security Considerations, Transport Level Security, HTTPS, SSH. **IP Security:** IP Security Overview, IP Security Policy, Encapsulating Security Payload, Authentication Header Protocol. **Electronic-Mail Security:** Internet-mail Security, Email Format, Email Threats and Comprehensive Email Security, S/MIME, PGP.

Text Books:

1. Cryptography and Network Security - Principles and Practice: William Stallings, Pearson Education, 7th Edition, 2017
2. Cryptography and Network Security: Behrouz A. Forouzan Debdeep, Mc Graw Hill, 3rd Edition, 2015

Reference Books:

1. Cryptography and Network Security: Atul Kahate, Mc Graw Hill, 3rd Edition
2. Introduction to Cryptography with Coding Theory: Wade Trappe, Lawrence C. Washington, Pearson.
3. Modern Cryptography: Theory and Practice By Wenbo Mao. Pearson



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

	BLOCKCHAIN TECHNOLOGY	L	T	P	C
		3	0	0	3

Course Objectives:

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

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, 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.



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

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 Hyperledger Fabric Network, Chain codes from Developer.ibm.com, Blockchain Application Using Fabric Java SDK.

Text book:

1. “Block chain Technology”, Chandramouli Subramanian, Asha A.George, Abhilash K A and Meena Karthikeyan , Universities Press.

Reference Books:

1. Blockchain Blue print for Economy, Melanie Swan, SPD Oreilly.
2. Blockchain for Business, Jai Singh Arun, Jerry Cuomo, Nitin Gauar, Pearson Addition Wesley



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

	CLOUD COMPUTING	L	T	P	C
		3	0	0	3

Course Objectives:

- To explain the evolving utility computing model called cloud computing.
- To introduce the various levels of services offered by cloud.
- To discuss the fundamentals of cloud enabling technologies such as distributed computing, service-oriented architecture and virtualization.
- To emphasize the security and other challenges in cloud computing.
- To introduce the advanced concepts such as containers, serverless computing and cloud-centric Internet of Things.

UNIT -I

Introduction to Cloud Computing Fundamentals, Cloud computing at a glance, defining a cloud, cloud computing reference model, types of services (IaaS, PaaS, SaaS), cloud deployment models (public, private, hybrid), utility computing, cloud computing characteristics and benefits, cloud service providers (Amazon Web Services, Microsoft Azure, Google AppEngine).

UNIT-II

Cloud Enabling Technologies, Ubiquitous Internet, parallel and distributed computing, elements of parallel computing, hardware architectures for parallel computing (SISD, SIMD, MISD, MIMD), elements of distributed computing, Inter-process communication, technologies for distributed computing, remote procedure calls (RPC), service-oriented architecture (SOA), Web services, virtualization.

UNIT-III

Virtualization and Containers, Characteristics of virtualized environments, taxonomy of virtualization techniques, virtualization and cloud Computing, pros and cons of virtualization, technology examples (XEN, VMware), building blocks of containers, container platforms (LXC, Docker), container orchestration, Docker Swarm and Kubernetes, public cloud VM (e.g. Amazon EC2) and container (e.g. Amazon Elastic Container Service) offerings.



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

UNIT-IV

Cloud computing challenges, Economics of the cloud, cloud interoperability and standards, scalability and fault tolerance, energy efficiency in clouds, federated clouds, cloud computing security, fundamentals of computer security, cloud security architecture, cloud shared responsibility model, security in cloud deployment models.

UNIT -V

Advanced concepts in cloud computing, Serverless computing, Function-as-a-Service, serverless computing architecture, public cloud (e.g. AWS Lambda) and open-source (e.g. OpenFaaS) serverless platforms, Internet of Things (IoT), applications, cloud-centric IoT and layers, edge and fog computing, DevOps, infrastructure-as-code, quantum cloud computing.

Text Books:

1. Mastering Cloud Computing, 2nd edition, RajkumarBuyya, Christian Vecchiola, ThamaraiSelvi, ShivanandaPoojara, Satish N. Srirama, McGraw Hill, 2024.
2. Distributed and Cloud Computing, Kai Hwang, Geoffery C. Fox, Jack J. Dongarra, Elsevier, 2012.

Reference Books:

1. Cloud Computing, Theory and Practice, Dan C Marinescu, 2nd edition, MK Elsevier, 2018.
2. Essentials of cloud Computing, K. Chandrasekhran, CRC press, 2014.
3. Online documentation and tutorials from cloud service providers (e.g., AWS, Azure, GCP)



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

	CYBER SECURITY LAB	L	T	P	C
		0	0	3	1.5

Course Objective: To get practical exposure to Cybersecurity threats and Forensics tools.

Course Outcome:

- Get the skill to identify cyber threats/attacks.
- Get the knowledge to solve security issues in day-to-day life.
- Able to use Autopsy tools
- Perform Memory capture and analysis
- Demonstrate Network analysis using Network miner tools

List of Experiments:

1. Perform an Experiment for port scanning with nmap
2. Set up a honeypot and monitor the honeypot on the network
3. Install Jscript/Cryptool tool (or any other equivalent) and demonstrate Asymmetric, Symmetric crypto algorithm, Hash and Digital/PKI signatures.
4. Generate minimum 10 passwords of length 12 characters using openSSL command
5. Perform practical approach to implement Footprinting - Gathering target information using Dmitry-Dmagic, UA tester
6. Work with sniffers for monitoring network communication (Wireshark).
7. Using Snort, perform real-time traffic analysis and packet logging.
8. Perform email analysis using the Autopsy tool.
9. Perform Registry analysis and get boot time logging using process monitor tool
10. Perform File type detection using Autopsy tool
11. Perform Memory capture and analysis using FTK imager tool
12. Perform Network analysis using the Network Miner 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.



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

	CRYPTOGRAPHY & NETWORK SECURITY LAB	L	T	P	C
		0	0	3	1.5

Course Objectives:

- To learn basic understanding of cryptography, how it has evolved, and some key encryption techniques used today.
- To understand and implement encryption and decryption using Ceaser Cipher, Substitution Cipher, Hill Cipher.

List of Experiments:

1. Write a C program that contains a string (char pointer) with a value 'Hello World'. The program should XOR each character in this string with 0 and displays the result.
2. Write a C program that contains a string (char pointer) with a value 'Hello World'. The program should AND or and XOR each character in this string with 127 and display the result
3. Write a Java program to perform encryption and decryption using the following algorithms:
 - a) Ceaser Cipher
 - b) Substitution Cipher
 - c) Hill Cipher
4. Write a Java program to implement the DES algorithm logic
5. Write a C/JAVA program to implement the BlowFish algorithm logic
6. Write a C/JAVA program to implement the Rijndael algorithm logic.
7. Using Java Cryptography, encrypt the text "Hello world" using BlowFish. Create your own key using Java key tool.
8. Write a Java program to implement RSA Algorithm
9. Implement the Diffie-Hellman Key Exchange mechanism using HTML and JavaScript. Consider the end user as one of the parties (Alice) and the JavaScript application as other party (bob).
10. Calculate the message digest of a text using the SHA-1 algorithm in JAVA.



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

OPEN ELECTIVES

	JAVA PROGRAMMING	L	T	P	C
		3	0	0	3

Course Objectives:

The learning objectives of this course are to:

- Identify language components and how they work to get her in applications
- Learn the fundamentals of object-oriented programming in Java, including defining classes, invoking methods, using class libraries.
- Learn how to extend Java classes with inheritance and dynamic binding and how to use exception handling in Java applications
- Understand how to design applications with threads in Java
- Understand how to use Java APIs for program development

UNIT I

Object Oriented Programming: Basic concepts, Principles, Program Structure in Java: Introduction, Writing Simple Java Programs, Elements or Tokens in Java Programs, Java Statements, Command Line Arguments, User Input to Programs, Escape Sequences Comments, Programming Style.

Data Types, Variables, and Operators :Introduction, Data Types in Java, Declaration of Variables, Data Types, Type Casting, Scope of Variable Identifier, Literal Constants, Symbolic Constants, Formatted Output with printf() Method, Static Variables and Methods, Attribute Final, **Introduction to Operators**, Precedence and Associativity of Operators, Assignment Operator (=), Basic Arithmetic Operators, Increment (++) and Decrement (- -) Operators, Ternary Operator, Relational Operators, Boolean Logical Operators, Bitwise Logical Operators. **Control Statements:** Introduction, if Expression, Nested if Expressions, if–else Expressions, Ternary Operator ?:, Switch Statement, Iteration Statements, while Expression, do–while Loop, for Loop, Nested for Loop, For-Each for Loop, Break Statement, Continue Statement.

UNIT II

Classes and Objects: Introduction, Class Declaration and Modifiers, Class Members, Declaration of Class Objects, Assigning One Object to Another, Access Control for Class Members, Accessing Private Members of Class, Constructor Methods for Class, Overloaded ConstructorMethods, NestedClasses, FinalClassandMethods, Passing ArgumentsbyValue and by Reference, Keyword this. **Methods:** Introduction, Defining Methods, Overloaded Methods, Overloaded Constructor Methods, Class Objects as Parameters in Methods, Access Control, Recursive Methods, Nesting of Methods, Overriding Methods, Attributes Final and Static.



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

UNIT III

Arrays: Introduction, Declaration and Initialization of Arrays, Storage of Array in Computer Memory, Accessing Elements of Arrays, Operations on Array Elements, Assigning Array to Another Array, Dynamic Change of Array Size, Sorting of Arrays, Search for Values in Arrays, Class Arrays, Two-dimensional Arrays, Arrays of Varying Lengths, Three-dimensional Arrays, Arrays as Vectors. **Inheritance:** Introduction, Process of Inheritance, Types of Inheritances, Universal Super Class-Object Class, Inhibiting Inheritance of Class Using Final, Access Control and Inheritance, Multilevel Inheritance, Application of Keyword Super, Constructor Method and Inheritance, Method Overriding, Dynamic Method Dispatch, Abstract Classes, Interfaces and Inheritance. **Interfaces:** Introduction, Declaration of Interface, Implementation of Interface, Multiple Interfaces, Nested Interfaces, Inheritance of Interfaces, Default Methods in Interfaces, Static Methods in Interface, Functional Interfaces, Annotations.

UNIT IV

Packages and Java Library: Introduction, Defining Package, Importing Packages and Classes into Programs, Path and Class Path, Access Control, Packages in Java SE, Java.lang Package and its Classes, Class Object, Enumeration, class Math, Wrapper Classes, Auto-boxing and Auto-unboxing, Java util Classes and Interfaces, Formatter Class, RandomClass, Time Package, Class Instant (java.time.Instant), Formatting for Date/Time in Java, Temporal Adjusters Class, Temporal Adjusters Class. **Exception Handling:** Introduction, Hierarchy of Standard Exception Classes, Keywords throws and throw, try, catch, and finally Blocks, Multiple Catch Clauses, Class Throwable, Unchecked Exceptions, Checked Exceptions.

Java I/O and File: Java I/O API, standard I/O streams, types, Byte streams, Character streams, Scanner class, Files in Java (Text Book 2)

UNIT V

String Handling in Java: Introduction, Interface Char Sequence, Class String, Methods for Extracting Characters from Strings, Comparison, Modifying, Searching; Class String Buffer. **Multithreaded Programming:** Introduction, Need for Multiple Threads Multithreaded Programming for Multi-core Processor, Thread Class, Main Thread-Creation of New Threads, Thread States, Thread Priority-Synchronization, Deadlock and Race Situations, Inter-thread Communication-Suspending, Resuming, and Stopping of Threads. **Java Database Connectivity:** Introduction, JDBC Architecture, Installing MySQL and MySQL Connector/J, JDBC Environment Setup, Establishing JDBC Database Connections, Result Set Interface. **Java FX GUI:** Java FX Scene Builder, Java FX App Window Structure, displaying text and image, event handling, laying out nodes in scene graph, mouse events (Text Book 3)



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

TextBooks:

1. JAVAonestepahead, AnithaSeth, B.L.Juneja,Oxford.
2. Joy with JAVA,Fundamentals of Object Oriented Programming, Debasis Samanta, Monalisa Sarma, Cambridge, 2023.
3. JAVA9forProgrammers,PaulDeitel,HarveyDeitel,4thEdition,Pearson.

ReferencesBooks:

1. ThecompleteReferenceJava,11thedition,HerbertSchildt,TMH
2. IntroductiontoJava programming, 7thEdition, YDanielLiang, Pearson

Online Resources:

1. <https://nptel.ac.in/courses/106/105/106105191/>
2. https://infyspringboard.onwingspan.com/web/en/app/toc/lex_auth_012880464547618816347_shared/overview



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

	OPERATING SYSTEMS	L	T	P	C
		3	0	0	3

Course Objectives:

The main objectives of the course is to make student

- Understand the basic concepts and principles of operating systems, including process management, memory management, file systems, and Protection
- Make use of process scheduling algorithms and synchronization techniques to achieve better performance of a computer system.
- Illustrate different conditions for dead lock and their possible solutions.

UNIT-I

Operating Systems Overview: Introduction, Operating system functions, Operating systems operations, Computing environments, Free and Open-Source Operating Systems

System Structures: Operating System Services, User and Operating-System Interface, system calls, Types of System Calls, system programs, Operating system Design and Implementation, Operating system structure, Building and Booting an Operating System, Operating system debugging

UNIT-II

Processes: Process Concept, Process scheduling, Operations on processes, Inter-process communication. **Threads and Concurrency:** Multithreading models, Thread libraries, Threading issues. **CPU Scheduling:** Basic concepts, Scheduling criteria,

Scheduling algorithms, Multiple processor scheduling.

UNIT- III

Synchronization Tools: The Critical Section Problem, Peterson's Solution, Mutex Locks, Semaphores, Monitors, Classic problems of Synchronization. **Deadlocks:**

system Model, Deadlock characterization, Methods for handling Deadlocks, Deadlock prevention, Deadlock avoidance, Deadlock detection, Recovery from Deadlock.

UNIT-IV

Memory-Management Strategies: Introduction, Contiguous memory allocation, Paging, Structure of the Page Table, Swapping. **Virtual Memory Management:**

Introduction, Demand paging, Copy-on-write, Page replacement, Allocation of frames, Thrashing. **Storage Management:** Overview of Mass Storage Structure, HDD Scheduling.



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

UNIT-V

File System: File System Interface: File concept, Access methods, Directory Structure; File system Implementation: File-system structure, File-system Operations, Directory implementation, Allocation method, Free space management; File-System Internals: File- System Mounting, Partitions and Mounting, File Sharing. **Protection:** Goals of protection, Principles of protection, Protection Rings, Domain of protection, Access matrix.

TextBooks:

1. Operating System Concepts, Silberschatz A, Galvin P B, Gagne G, 10th Edition, Wiley, 2018.
2. ModernOperatingSystems,TanenbaumAS,4thEdition,Pearson,2016

ReferenceBooks:

1. OperatingSystems-InternalsandDesignPrinciples,StallingsW,9thedition, Pearson, 2018
2. OperatingSystems:AConceptBasedApproach,D.MDhamdhere,3rdEdition, McGraw- Hill, 2013

OnlineLearningResources:

1. <https://nptel.ac.in/courses/106/106/106106144/>
- <http://peterindia.net/OperatingSystems.html>



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

	DATABASE MANAGEMENT SYSTEMS	L	T	P	C
		3	0	0	3

Course Objectives:

The main objectives of the course is to

- Introduce database management systems and to give a good formal foundation on the relational model of data and usage of Relational Algebra
- Introduce the concepts of basic SQL as a universal Data base language
- Demonstrate the principles behind systematic data base design approaches by covering conceptual design, logical design through normalization
- Provide an overview of physical design of a database system, by discussing Database indexing techniques and storage techniques

UNIT-I

Introduction: Database system, Characteristics (Database Vs File System), Database Users, Advantages of Database systems, Database applications. Brief introduction of different Data Models; Concepts of Schema, Instance and data independence; Three-tier schema architecture for data independence; Database system structure, environment, Centralized and Client Server architecture for the database.

Entity Relationship Model: Introduction, Representation of entities, attributes, entity set, relationship, relationship set, constraints, sub classes, super class, inheritance, specialization, generalization using ER Diagrams.

UNIT-II

Relational Model: Introduction to relational model, concepts of domain, attribute, tuple, relation, importance of null values, constraints (Domain, Key constraints, integrity constraints) and their importance, Relational Algebra, Relational Calculus. BASICSQL: Simple Databases schema, data types, table definitions (create, alter), different DML operations (insert, delete, update).

UNIT-III

SQL: Basic SQL querying (select and project) using where clause, arithmetic & logical operations, SQL functions (Date and Time, Numeric, String conversion). Creating tables with relationships, implementation of key and integrity constraints, nested queries, sub queries, grouping, aggregation, ordering, implementation of different types of joins, view (updatable and non-updatable), relational set operations.



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

UNIT-IV

Schema Refinement (Normalization): Purpose of Normalization or schema refinement, concept of functional dependency, normal forms based on functional dependency Loss less join and dependency preserving decomposition, (1NF, 2NF and 3NF), concept of surrogate key, Boyce-Codd normal form (BCNF), MVD, Fourth normal form (4NF), Fifth Normal Form (5NF).

UNIT-V

Transaction Concept: Transaction State, ACID properties, Concurrent Executions, Serializability, Recoverability, Implementation of Isolation, Testing for Serializability, lock based, time stamp based, optimistic, concurrency protocols, Deadlocks, Failure Classification, Storage, Recovery and Atomicity, Recovery algorithm.

Introduction to Indexing Techniques: B+ Trees, operations on B+Trees, Hash Based Indexing:

Text Books:

- 1) Database Management Systems, 3rd edition, Raghurama Krishnan, Johannes Gehrke, TMH (For Chapters 2, 3, 4)
- 2) Database System Concepts, 5th edition, Silberschatz, Korth, Sudarsan, TMH (For Chapter 1 and Chapter 5)

Reference Books:

- 1) Introduction to Data base Systems, 8th edition, CJ Date, Pearson.
- 2) Database Management System, 6th edition, Ramez Elmasri, Shamkant B. Navathe, Pearson
- 3) Database Principles Fundamentals of Design Implementation and Management, Corlos Coronel, Steven Morris, Peter Robb, Cengage Learning.

Web-Resources:

- 1) <https://nptel.ac.in/courses/106/105/106105175/>
- 2) https://infyspringboard.onwingspan.com/web/en/app/toc/lex_auth_01275806667282022456_shared/overview



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA
KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security
(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

	COMPUTER NETWORKS	L	T	P	C
		3	0	0	3

Course Objectives:

- To understand the different types of networks
- To discuss the software and hardware components of a network
- To develop an understanding the principles of computer networks.
- To familiarize with OS Model and the function so layered structure.
- To explain networking protocols, algorithms and design perspectives.

CourseOutcomes(CO):

After completion of the course, students will be able to

- Identify the software and hardware components of a Computer network.(L1)
- Explain the functionality of each layer of a computer network.(L2)
Identify and analyze flow control, congestion control, and routing issues.(L4)
- Analyze and interpret the functionality and effectiveness of the routing protocols.
(L4)
- Choose the appropriate transport protocol based on the application requirements.(L3)

UNIT-I

Introduction: Types of Computer Networks, Broadband Access Networks, Mobile and Wireless Access Networks, Content Provider Networks, Transit networks, Enterprise Networks, Network technology from local to global, Personal Area Networks, Local Area Networks, Home Networks, Metropolitan Area Networks, Wide Area Networks, Internetworks, Network Protocols, Design Goals, Protocol Layering, Connections and Reliability, Service Primitives, The Relationship of Services to Protocols ,Reference Models, The OSI Reference Model, The TCP/IP Reference Model, A Critique of the OSI Model and Protocols, A Critique of the TCP/IP Reference Model and Protocols.

UNIT-II

The Data Link Layer: Guided Transmission Media, Persistent Storage, Twisted Pairs, CoaxialCable, PowerLines, Fiber Optics, Data Link Layer DesignIssues, Services Provided To The Network Layer, Framing Error Control, Flow Control, Error Detection And Correction, Error-Correcting Codes, Error-Detecting Codes, Elementary Data Link Protocols, Initial Simplifying Assumptions Basic Transmission And Receipt, Simplex Link-Layer Protocols, Improving Efficiency, Bidirectional Transmission, Multiple Frames In Flight, Examples Of Full-Duplex, Sliding Window Protocols, The Channel Allocation Problem, Static Channel Allocation, AssumptionsForDynamicChannelAllocation, MultipleAccessProtocols, Aloha, Carrier Sense Multiple Access Protocols, Collision-Free Protocols, Limited-Contention Protocols, Wireless LAN Protocols, Ethernet, Classic Ethernet Physical Layer, Classic Ethernet Mac Sublayer Protocol, Ethernet Performance, Switched Ethernet, Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet, 40- And 100-Gigabit Ethernet, Retrospective On Ethernet.



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA–533003, Andhra Pradesh, India

R23 B.Tech Cyber Security

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

UNIT-III

The Network Layer: Network Layer Design Issues, Store-And-Forward Packet Switching, Services Provided To The Transport Layer, Implementation Of Connectionless Service, Implementation Of Connection-Oriented Service, Comparison Of Virtual-Circuit And Datagram Networks, Routing Algorithms In A Single Network, The Optimality Principle, Shortest Path Algorithm, Flooding, Distance Vector Routing, Link State Routing, Hierarchical Routing Within a Network, Broadcast Routing, Multicast Routing, Anycast Routing, Traffic Management at The Network Layer, The Need for Traffic Management: Congestion, Approaches To Traffic Management, Internetworking, Internetworks: An Overview, How Networks differ, Connecting Heterogeneous Networks, Connecting Endpoints Across Heterogeneous Networks, Internetwork Routing: Routing Across Multiple Networks Supporting Different Packet Sizes:Packet Fragmentation,The Network Layer In The Internet, The IP Version 4 Protocol, IP Addresses, IP Version 6, Internet Control Protocols, Label Switching and MPLS, OSPF—An Interior Gateway Routing Protocol, BGP—The Exterior Gateway Routing Protocol, Internet Multicasting.

UNIT-IV

The Transport Layer: The Transport Service, Services Provided To The Upper Layers, Transport Service Primitives, Berkeley Sockets, An Example Of Socket Programming: An Internet File Server, Elements Of Transport Protocols, Addressing, Connection Establishment, Connection Release, Error Control And Flow Control, Multiplexing, Crash Recovery, Congestion Control, Desirable Band width Allocation, Regulating The Sending Rate,Wireless Issues, The Internet Transport Protocols: UDP, Introduction To UDP, Remote Procedure Call, Real-Time Transport Protocols, The Internet Transport Protocols:TCP,IntroductionToTCP, The TCP Service Model, The TCP Protocol, The TCP Segment Header, TCP Connection Establishment, TCP Connection Release.

UNIT-V

The Application Layer: Electronic Mail, Architecture and Services, The User Agent, Message Formats, Message Transfer, Final Delivery, The World Wide Web, Architectural Overview, Static Web Objects, Dynamic Web Pages and Web Applications, HTTP and HTTPS, Web Privacy, Content Delivery, Content and Internet Traffic, Server Farms and Web Proxies, Content Delivery Networks, Peer-To-Peer Networks, Evolution of The Internet.



JAWAHARLALNEHRUTECHNOLOGICALUNIVERSITY KAKINADA

(Established by Govt. of A.P., ACT No. 30 of 2008)

KAKINADA – 533003 (A.P) INDIA

Textbook:

1. Andrew Tanenbaum, Feamster Wetherall, Computer Networks, 6th Edition, Global Edition.

Reference Books:

1. Behrouz A. Forouzan, Data Communications and Networking, 5th Edition, McGraw Hill Publication, 2017.
2. James F. Kurose, Keith W. Ross, "Computer Networking: A Top-Down Approach", 6th edition, Pearson, 2019.
3. Youlu Zheng, Shakil Akthar, "Networks for Computer Scientists and Engineers", Oxford Publishers, 2016.

Online Learning Resources:

<https://nptel.ac.in/courses/106105183/25>
<http://www.nptelvideos.in/2012/11/computer-networks.html> <https://nptel.ac.in/courses/106105183/>