



School of Computer Science & IT Devi Ahilya Vishwavidyalaya

SYLLABUS

M.Tech (Network Management & Information Security) 2 years

Program Educational Objectives (PEOs)

- PEO 1:** Acquire practical knowledge in Network Management & Information Security and pursue careers as a network administrator or information security expert.
- PEO 2:** Demonstrate ability to administer state-of-the-art computer networks.
- PEO 3:** Build foundation to perform research in related domains and pursue successful careers in academia.

Program Specific Outcomes (PSOs)

- PSO 1:** Acquire knowledge of networking technologies and apply that knowledge to manage real computer networks using cutting edge network management tools.
- PSO 2:** Develop knowledge of security fundamentals and leverage that knowledge to ensure information security of an organization.

II - SEMESTER

CS-4524: LINUX ESSENTIALS FOR CYBER SECURITY

Course Outcomes (COs):

- CO1:** Understand Linux architecture, file systems, and basic administration tasks.
- CO2:** Operate effectively on the Linux command line for system and security tasks.
- CO3:** Use shell scripting for automation and cybersecurity operations.
- CO4:** Apply Linux networking and user management for secure environments.
- CO5:** Configure, audit, and harden Linux systems against cyber threats using Kali Linux tools.
-

Course Contents

- UNIT-I** **No. of Hours: 6**
Linux Fundamentals & Architecture: Introduction to Linux and Open Source Philosophy, Linux Distributions and File Hierarchy, Structure, Linux Boot Process and System Initialization, Basic Shell and Terminal Operations, File and Directory Management (ls, cp, mv, rm, chmod, chown, ln), Understanding File Permissions and Ownership, Package Management (apt, yum, dnf).
- UNIT-II** **No. of Hours: 6**
Command-Line Mastery & Shell Scripting: Essential Commands for Cybersecurity Experts, Environment Variables and Shell Configuration Files, Bash Shell Scripting Fundamentals, Conditional Statements and Loops, Functions and Script Parameters, Writing Automation Scripts for Log Monitoring, Backup, and System Tasks, Cron Jobs and Task Scheduling.
- UNIT-III** **No. of Hours: 6**
User, File, and Process Management for Security: User and Group Administration (useradd, passwd, groupmod, sudoers), File Permissions, ACLs, and Secure Access Controls, Process Monitoring and Management (ps, top, kill, nice, renice), Resource Monitoring (df, du, free, vmstat, iostat), Log Management (rsyslog, journalctl, /var/log), Securing the Linux File System, Configuring and Managing Firewalls (ufw, iptables basics).
- UNIT-IV** **No. of Hours: 6**
Networking and System Security in Linux: Linux Networking Fundamentals (ifconfig, ip, netstat, ss, ping, traceroute), Network Configuration and Troubleshooting, Secure Shell (SSH) Configuration and Key-based Authentication, Configuring Firewalls with iptables and ufw, Intrusion Detection Concepts (auditd, fail2ban) System Hardening Techniques, Introduction to Linux Security Modules (SELinux, AppArmor).
- UNIT-V** **No. of Hours: 6**
Linux for Ethical Hacking and Security Operations: Introduction to Kali Linux and Security-Focused Distributions, File Integrity and Log Auditing Tools, Linux Command-Line Tools for Reconnaissance (nmap, netcat, tcpdump), Password Auditing and User Security (John the Ripper, Hydra), Privilege

Escalation Techniques and Mitigation, Forensics Basics using Linux Tools, Hardening Linux for Penetration Testing Environments.

Text Books:

1. Linux: The Complete Reference, McGraw-Hill Education, Richard Petersen, 6th Edition, 2022.
2. The Linux Command Line: A Complete Introduction, William E. Shotts, Jr. No Starch Press, 2nd Edition, 2019.
3. Linux Basics for Hackers: Getting Started with Networking, Scripting, and Security in Kali, OccupyTheWeb, No Starch Press, 2018.

Reference Books:

1. Linux Command Line and Shell Scripting Bible, Christine Bresnahan & Richard Blum, Wiley, 4th Edition, 2021.
2. Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort, Michael Rash, No Starch Press, 2017.
3. LPIC-1: Linux Professional Institute Certification Study Guide, Roderick W. Smith, Wiley, 5th Edition, 2022.

Online Resources:

1. <https://training.linuxfoundation.org/resources/>
2. <https://www.kali.org/docs/>
3. <https://help.ubuntu.com/>

CS-4524: LINUX ESSENTIALS FOR CYBER SECURITY- PRACTICAL

Course Outcomes (COs):

CO1: Understand the principles and concepts of computer forensics.

CO2: Develop skills in conducting computer investigations using a systematic approach.

CO3: Gain proficiency in acquiring and preserving digital evidence from different storage formats.

CO4: Explore the use of specialized tools and software for computer forensics analysis.

CO5: Analyze techniques for investigating network-related incidents and conducting live acquisitions.

Course Contents

UNIT-I

No. of Hours: 8

1. Create a Forensic Image using FTK Imager/Encase Imager (Creating Forensic Image, Check Integrity of Data, Analyze Forensic Image).
2. Perform data acquisition using USB Write Blocker + Encase Imager, SATA Write Blocker + Encase Imager, Falcon Imaging Device.
3. Analyze the memory dump of a running computer system (Extract volatile data, such as open processes, network connections, and registry information).

UNIT-II

No. of Hours: 8

1. Recovering and Inspecting deleted files (Check for Deleted Files, Recover the Deleted Files, Analyzing and Inspecting the recovered files, Perform this using recovery option in EnCase and also Perform manually through Command line).
2. Demonstrate restoring of Evidence Image using EnCase Forensics.
3. Monitoring Activity Log (Last activity of Your PC).
4. Find Last Connected USB on your system (USB Forensics).

UNIT-III

No. of Hours: 8

1. Capturing and analyzing network packets using Wireshark (Identification the live network, Capture Packets, Analyze the captured packets).
2. Using Sysinternals tools for Network Tracking and Process Monitoring (Check Sysinternals tools, Monitor Live Processes, Capture RAM, Capture TCP/UDP packets, Monitor Hard Disk,. Monitor Virtual Memory, Monitor Cache Memory).

UNIT-IV

No. of Hours: 8

1. Demonstration of Steganography (Detect hidden information or files within digital images using steganography analysis tools, Extract and examine the hidden content).
2. Email Forensics (Analyze email headers and content to trace the origin of suspicious emails, Identify potential email forgeries or tampering).

UNIT-V**No. of Hours: 8**

1. Perform forensic analysis for mobile device, such as a smartphone or tablet, Retrieve call logs, text messages, and other relevant data for investigative purposes (Mobile device forensics).
2. Analyze browser artifacts, including history files, bookmarks, and download records, Analyze cache and cookies data to reconstruct user-browsing history and identify visited websites or online activities (Web Browser Forensics).
3. Extract the relevant log or timestamp file, analyze its contents and interpret the timestamp data to determine the user's last internet activity and associated details.

Text Books:

1. Linux: The Complete Reference, McGraw-Hill Education, Richard Petersen, 6th Edition, 2022.
2. The Linux Command Line: A Complete Introduction, William E. Shotts, Jr. No Starch Press, 2nd Edition, 2019.
3. Linux Basics for Hackers: Getting Started with Networking, Scripting, and Security in Kali, OccupyTheWeb, No Starch Press, 2018.

Reference Books:

1. Linux Command Line and Shell Scripting Bible, Christine Bresnahan & Richard Blum, Wiley, 4th Edition, 2021.
2. Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort, Michael Rash, No Starch Press, 2017.
3. LPIC-1: Linux Professional Institute Certification Study Guide, Roderick W. Smith, Wiley, 5th Edition, 2022.

Online Resources:

1. <https://training.linuxfoundation.org/resources/>
2. <https://www.kali.org/docs/>
3. <https://help.ubuntu.com/>

CS-5618: NETWORK SECURITY

Course Outcomes (COs):

CO1: Explain basic communication networks, security goals, and network attacks.

CO2: Analyze mechanisms for message integrity, authentication, and non-repudiation.

CO3: Describe authentication frameworks, PKI, and digital certificates.

CO4: Apply network, transport, wireless, and perimeter security mechanisms.

CO5: Evaluate emerging security technologies and future cybersecurity challenges.

Course Contents

UNIT-I

No. of Hours: 8

Fundamentals of Network Security: Introduction to communication networks and their role in modern information systems. Review of basic networking concepts and architectures. Introduction to network security: objectives, principles, and security goals. Classification of network threats and vulnerabilities. Types of attacks on networks including passive and active attacks. Common network attacks such as eavesdropping, spoofing, replay attacks, man-in-the-middle attacks, denial-of-service, and distributed denial-of-service attacks. Impact of network attacks on confidentiality, integrity, and availability.

UNIT-II

No. of Hours: 8

Message Protection and Data Integrity Mechanisms: Message integrity and data authentication concepts. Cryptographic hash functions and their properties. Secure message digest generation and verification. Digital signatures: concept, working principles, and applications in secure communication, electronic transactions, and authentication systems. Role of integrity and non-repudiation in secure networked environments.

UNIT-III

No. of Hours: 8

Authentication and Key Management Infrastructure: Introduction to authentication and access control. Authentication principles and security requirements. Entity authentication and message authentication mechanisms. Role of trust in secure systems. Public Key Infrastructure (PKI): architecture and components. Digital certificates and their purpose. Certificate authorities and trust models. Certificate issuance, validation, renewal, and revocation. Role of PKI in secure electronic transactions and communications.

UNIT-IV

No. of Hours: 8

Network and Wireless Security Mechanisms: Introduction to security at different network layers. Transport Layer Security (TLS): objectives and basic working principles. Network layer security mechanisms. Virtual Private Networks (VPNs): concepts, types, and applications. Security issues and solutions in Wireless Local Area Networks (WLANs). Wireless cellular network security and associated challenges. Firewalls: types, architectures, and deployment strategies. Intrusion

Detection Systems (IDS) and Intrusion Prevention Systems (IPS): concepts, types, and operational principles.

UNIT-V

No. of Hours: 8

Emerging Security Technologies and Advanced Topics: Introduction to cryptocurrencies and blockchain technology. Fundamental concepts of blockchain architecture and security features. Cloud computing security: threats, vulnerabilities, and protection mechanisms. Security challenges in the Internet of Things (IoT). Hardware security concepts and trusted hardware components. Anonymous communication systems and privacy preservation. Onion routing and anonymous network communication. Introduction to post-quantum cryptography and future challenges in cryptographic security.

Text Books:

1. Network Security: Private Communication in a Public World, C. Kaufman, R. Perlman, M. Speciner, R. Perlner, Pearson Education, 3rd Edition, 2024.
2. Computer Networking: A Top Down Approach, J. Kurose, K. Ross, Pearson Education, 8th Edition, 2022.

Reference Books:

1. Cryptography, Network Security, and Cyber Laws, B. L. Menezes, R. Kumar, Cengage Learning India Pvt. Ltd., 2018.
2. Real 802.11 Security: Wi Fi Protected Access and 802.11i, J. Edney, W. A. Arbaugh, Pearson Education, 2004.
3. Cryptography and Network Security: Principles and Practice, W. Stallings, Pearson Education, 8th Edition, 2023.
4. Computer Networks: A Systems Approach, L. Peterson, B. Davie, Morgan Kaufmann, 6th Edition, 2021.

Online Resources:

1. https://onlinecourses.nptel.ac.in/noc26_ee20/preview

CS-5618: NETWORK SECURITY- PRACTICAL

Course Outcomes (COs):

CO1: Analyze network traffic and identify common network attacks.

CO2: Implement data integrity and non-repudiation using cryptographic tools.

CO3: Apply authentication mechanisms and manage digital certificates.

CO4: Configure and evaluate network, wireless, and perimeter security solutions.

CO5: Explore emerging cybersecurity technologies through case studies and projects.

Course Contents

UNIT-I

No. of Hours: 6

Fundamentals of Network Security:

1. Study of basic network configurations using TCP/IP tools.
2. Packet capturing and analysis using Wireshark.
3. Identification and analysis of common network attacks (e.g., sniffing, spoofing, DoS) in a controlled environment.
4. Demonstration of network vulnerability scanning using standard tools.

UNIT-II

No. of Hours: 6

Message Protection and Data Integrity Mechanisms:

1. Generation and verification of cryptographic hash values using standard hash algorithms.
2. Demonstration of digital signature creation and verification.
3. Integrity checking of transmitted files using hash-based techniques.
4. Case study–based analysis of integrity and non-repudiation failures.

UNIT-III

No. of Hours: 6

Authentication and Key Management Infrastructure:

1. Study of authentication mechanisms used in networked systems.
2. Creation and verification of digital certificates using a certificate authority tool.
3. Demonstration of certificate validation and revocation checking.
4. Analysis of PKI-based secure communication scenarios.

UNIT-IV

No. of Hours: 6

Network and Wireless Security Mechanisms:

1. Configuration and analysis of Transport Layer Security (TLS) connections.
2. Setup and testing of Virtual Private Network (VPN).
3. Configuration of firewall rules and traffic filtering.
4. Demonstration of Intrusion Detection System (IDS) alerts and logs.
5. Study of security mechanisms in WLANs and wireless networks.

UNIT-V**No. of Hours: 6**

Emerging Security Technologies and Advanced Topics:

1. Study of blockchain structure and transaction validation.
2. Case study on cloud security threats and mitigation strategies.
3. Analysis of security issues in IoT environments.
4. Demonstration of anonymous communication concepts using onion routing tools.
5. Seminar or mini-project on post-quantum cryptography or emerging security trends.

Text Books:

1. Network Security: Private Communication in a Public World, C. Kaufman, R. Perlman, M. Speciner, R. Perlner, Pearson Education, 3rd Edition, 2024.
2. Computer Networking: A Top Down Approach, J. Kurose, K. Ross, Pearson Education, 8th Edition, 2022.

Reference Books:

1. Cryptography, Network Security, and Cyber Laws, B. L. Menezes, R. Kumar, Cengage Learning India Pvt. Ltd., 2018.
2. Real 802.11 Security: Wi Fi Protected Access and 802.11i, J. Edney, W. A. Arbaugh, Pearson Education, 2004.
3. Cryptography and Network Security: Principles and Practice, W. Stallings, Pearson Education, 8th Edition, 2023.
4. Computer Networks: A Systems Approach, L. Peterson, B. Davie, Morgan Kaufmann, 6th Edition, 2021.

Online Resources:

1. https://onlinecourses.nptel.ac.in/noc26_ee20/preview

CS-6226: ADVANCED ALGORITHM DESIGN

Course Outcomes (COs):

CO1: Understand complexity representation in terms of asymptotic notations.

CO2: Apply different algorithm design paradigms such as divide-and-conquer, greedy and dynamic programming for effective problem-solving

CO3: Understand and analyse major graph algorithms.

CO4: Apply string matching algorithms.

CO5: Understand design paradigms such as backtracking, branch & bound and concept of complexity class.

Course Contents

UNIT-I

No. of Hours: 8

Introduction to Algorithms, Time & Space Complexity, Sorting: Merge Sort, Quick Sort, Heap Sort; Searching: Linear Search, Binary Search, Hashing.

UNIT-II

No. of Hours: 8

Greedy Techniques & its Applications: Fractional Knapsack, Activity Selection Problem
Dynamic Programming & its Applications: Fibonacci Computation, 0/1 Knapsack Problem, Longest Common Subsequence Problem, Edit Distance Problem; Matrix Chain Multiplication. Edit distance, All pair shortest paths – Warshal's and Floyd's algorithms.

UNIT-III

No. of Hours: 8

Graph Algorithms, Traversal: BFS, DFS; Shortest Path: Dijkstra's Shortest Path Algorithm; Computation of Minimum Spanning Trees: Prim Algorithm, Kruskal Algorithm.

UNIT-IV

No. of Hours: 8

String Matching Algorithms: Naïve Algorithm, KMP Algorithm, Rabin-Karp Algorithm.

UNIT-V

No. of Hours: 8

Backtracking: n-Queen Problem, Sum of Subset, Branch and Bound: Travelling Salesman Problem, Introduction to P, NP, NP-complete, NP-Hard.

Text Books:

1. Thomas H. Cormen, Charles E. Leiserson and Ronald L. Rivest (2022), Introduction to Algorithms, Fourth edition, Prentice Hall of India.
2. Ellis Horowitz, Sartaj Sahni, Sanguthevar Rajasekaran (2008), "Fundamentals of Computer Algorithms", Orient Longman Pvt. Ltd.

Reference Books:

1. Gilles Brassard Paul Bratley (1996), "Fundamentals of Algorithms", Prentice Hall.
2. Anany Levitin (2009), "An Introduction to Design and Analysis of Algorithms", Pearson.

Online Resources:

1. NPTEL Course Video Lectures on "Design and Analysis of Algorithms" - By Prof. Abhiram G Ranade, Prof. Ajit A Diwan, Prof. Sundar Viswanathan IIT Bombay
2. NPTEL Course Video Lectures on "Design and Analysis of Algorithms" - Prof. Madhavan Mukund, Chennai Mathematical Institute.

CS-6226: ADVANCED ALGORITHM DESIGN - PRACTICAL

Course Outcomes (COs):

CO1: Compare and analyse different data structures and sorting algorithms.

CO2: Analyse major graph algorithms.

CO3: Implement different algorithm design paradigms such as greedy, dynamic programming, backtracking, branch and bound for effective problem-solving.

CO4: Apply string matching algorithms.

CO5: Understand design paradigms such as backtracking, branch & bound and concept of complexity class.

Course Contents

UNIT-I

No. of Hours: 8

Implement the following sorting algorithm for a given set of elements and determine the time required to sort the elements. The elements can be read from a file or can be generated using the random number generator.

1. Quick sort
2. Merge sort
3. Heap Sort
4. Counting Sort

Implement the following Searching algorithm for a given set of elements and determine the time required to sort the elements. The elements can be read from a file or can be generated using the random number generator.

1. Linear Search,
2. Binary Search,
3. Hashing

UNIT-II

No. of Hours: 8

Write programs to find the optimal solution for the following problems using the Greedy Method

1. Fractional Knapsack
2. Activity Selection Problem.
3. Minimum Spanning trees – Prim's and Kruskal's algorithms.
4. Single-source shortest paths - Dijkstra's algorithms

UNIT-III

No. of Hours: 8

Write programs to find the optimal solution for the following problems using the Dynamic Programming approach

1. 0/1 Knapsack
2. Longest Common Subsequence (LCS)

3. Matrix Chain Multiplication
4. Edit distance
5. All pair shortest paths – Warshal’s and Floyd’s algorithms

UNIT-IV

No. of Hours: 8

Write programs to print all the nodes reachable from a given starting node in a graph using the following traversal methods

1. Breadth First Search (BFS)
2. Depth First Search (DFS)

Write programs to implement the following string matching algorithms:

1. Naïve Algorithm
2. KMP Algorithm,
3. Rabin-Karp Algorithm

UNIT-V

No. of Hours: 6

Write programs to find the optimal solution for the following problems using the Backtracking approach

1. Graph Coloring
2. Sum of Subset

Write a program to find the optimal solution for the following problems using the Branch and Bound method

1. Travelling Salesman Problem

Text Books:

1. Thomas H. Cormen, Charles E. Leiserson and Ronald L. Rivest (2022), Introduction to Algorithms, Fourth edition, Prentice Hall of India.
2. Ellis Horowitz, Sartaj Sahni, Sanguthevar Rajasekaran (2008), “Fundamentals of Computer Algorithms”, Orient Longman Pvt. Ltd.

Reference Books:

Online Resources:

1. NPTEL Course Video Lectures on “Design and Analysis of Algorithms” - By Prof. Abhiram G Ranade, Prof. Ajit A Diwan, Prof. Sundar Viswanathan IIT Bombay
2. NPTEL Course Video Lectures on “Design and Analysis of Algorithms” - Prof. Madhavan Mukund, Chennai Mathematical Institute.

CS-6518: CLOUD COMPUTING

Course Outcomes (COs):

- CO1:** Understand the concepts, key technologies, strengths, and limitations of cloud computing and the possible applications for state-of-the-art cloud computing
- CO2:** Understand the architecture and infrastructure of cloud computing, including SaaS, PaaS, IaaS, public cloud, private cloud, hybrid cloud, multicloud.
- CO3:** : Developing In-depth Knowledge of Cloud Service Models and Virtualization and design cloud computing solutions according to the application domain.
- CO4:** Implement IaaS, SaaS, PaaS through AWS, Google Cloud, Salesforce and other service providers.
- CO5:** Learn the core issues and latest trends and technologies of cloud computing.
-

Course Contents

UNIT-I

No. of Hours: 10

Cloud Computing definition, Types of cloud, Evolution of Cloud Computing, Applications cloud computing, Cluster Computing, Major Players in Cloud Computing, Issues and challenges in Cloud, Cloud stakeholders, SLAs, Economics of the Cloud
Cloud Models: Public Cloud, Private Cloud, Hybrid Cloud, Community Cloud. Advantages, disadvantages and applications of the deployment models.

UNIT-II

No. of Hours: 8

Basics of Virtualization, Types of Virtualization, Virtualization using virtualbox, Virtualization Tools and Mechanisms, Creating virtual machines in AWS, Virtualization for Data-center Automation, Scalability, Load balancing, Server Management, Fault Tolerance.

UNIT-III

No. of Hours: 12

Types of Cloud services: Infrastructure as a Service: Compute Services, clusters, HPC, Data Storage services and its categories- File storage, Block storage, Object storage, applications utilizing cloud storage, Network Services.
Platform as a Service: Understand and develop application using PaaS. Software as a Service: Applications, working, development methodology, advantages and disadvantages.

UNIT-IV

No. of Hours: 8

Database as a Service, Functions as a service-Serverless Computing, Microservices Introduction to MapReduce, HDFS, Hadoop Framework. Devops, Containers, Kubernetes.

UNIT-V

No. of Hours: 8

Security issues in cloud, AI and Machine Learning in Cloud, Fog Computing, Edge Computing, Green Cloud.
Case Studies:

Hypervisors – Xen, KVM , VMWare, Virtual Box, Hyper-V.

Cloud Service Providers- AWS, Microsoft Azure, Github, Google Workspace, Salesforce

Text Books:

1. Buyya, Rajkumar, Christian Vecchiola, and S. Thamarai Selvi. Mastering cloud computing: foundations and applications programming. Newnes, 2013.
2. Kai Hwang, Geoffrey C. Fox and Jack J. Dongarra, “Distributed and cloud computing from Parallel Processing to the Internet of Things”, Morgan Kaufmann, Elsevier – 2012

Reference Books:

1. Cloud Computing “A Practical Approach” Anthony T. Velte, Toby J. Velte, Robert Elsenpeter. McGraw-Hill.
2. Kai Hwang, Geoffrey C Fox, Jack G Dongarra, “Distributed and Cloud Computing, From Parallel Processing to the Internet of Things”, Morgan Kaufmann Publishers, 2012.
3. John W.Rittinghouse and James F.Ransome, “Cloud Computing: Implementation, Management, and Security”, CRC Press, 2010.
4. Toby Velte, Anthony Velte, Robert Elsenpeter, “Cloud Computing, A Practical Approach”, TMH, 2009.
5. Kumar Saurabh, “ Cloud Computing – insights into New -Era Infrastructure”, Wiley India,2011.

Online Resources:

1. <https://www.mygreatlearning.com/cloud-computing/free-courses>
2. <https://aws.amazon.com/training/digital/>
3. <https://www.simplilearn.com/introduction-to-cloud-computing-basics-skillup>
4. <https://www.geeksforgeeks.org/>
5. <https://www.javatpoint.com/>

CS-6518: CLOUD COMPUTING - PRACTICAL

Course Outcomes (COs):

- CO1:** Understand the concepts, key technologies, strengths, and limitations of cloud computing and the possible applications for state-of-the-art cloud computing.
- CO2:** Understand the architecture and infrastructure of cloud computing, including SaaS, PaaS, IaaS, public cloud, private cloud, hybrid cloud, multicloud.
- CO3:** Developing In-depth Knowledge of Cloud Service Models and Virtualization and design cloud computing solutions according to the application domain.
- CO4:** Implement IaaS, SaaS, PaaS through AWS, Google Cloud, Salesforce and other service providers.
- CO5:** Learn the core issues and latest trends and technologies of cloud computing.
-

Course Contents

UNIT-I

No. of Hours: 6

1. Install Virtualbox/VMware Workstation with different flavor of linux or windows OS on top of windows.
2. Install a C compiler in the virtual machine created using virtual box and execute Simple Programs.
3. Create a free account in AWS and create a virtual machine, configure it and run program on VM.

UNIT-II

No. of Hours: 4

1. Explore data storage, server management, cloud watch and load balancing tools of AWS. Attach data storage to VM.
2. Create account and explore the applications of GitHub.
3. Explore cloud platforms for Web Application development and Mobile App development.

UNIT-III

No. of Hours: 4

1. Create a website using Wordpress and host it on cloud.
2. Explore Google workspace.
3. Create a free account in Salesforce (if available) and explore its functionalities.

UNIT-IV

No. of Hours: 6

1. Develop a SAAS application in team and deploy it on cloud.
2. Explore microservices and serverless computing.
3. Understand DevOps concepts and implementation details. Write complete note on steps required for developing CI/CD pipelines.

UNIT-V

No. of Hours: 4

1. Explore security solutions in cloud.
2. Install Hadoop single node cluster and run simple applications like wordcount.
3. Study scalability through containerized applications and kubernetes.

Text Books:

1. Buyya, Rajkumar, Christian Vecchiola, and S. Thamarai Selvi. Mastering cloud computing: foundations and applications programming. Newnes, 2013.
2. Kai Hwang, Geoffrey C. Fox and Jack J. Dongarra, "Distributed and cloud computing from Parallel Processing to the Internet of Things", Morgan Kaufmann, Elsevier – 2012

Reference Books:

1. Cloud Computing "A Practical Approach" Anthony T. Velte, Toby J. Velte, Robert Elsenpeter. McGraw-Hill.
2. Kai Hwang, Geoffrey C Fox, Jack G Dongarra, "Distributed and Cloud Computing, From Parallel Processing to the Internet of Things", Morgan Kaufmann Publishers, 2012.
3. John W.Rittinghouse and James F.Ransome, "Cloud Computing: Implementation, Management, and Security", CRC Press, 2010.
4. Toby Velte, Anthony Velte, Robert Elsenpeter, "Cloud Computing, A Practical Approach", TMH, 2009.
5. Kumar Saurabh, " Cloud Computing – insights into New -Era Infrastructure", Wiley India,2011.

Online Resources:

1. <https://www.mygreatlearning.com/cloud-computing/free-courses>
2. <https://aws.amazon.com/training/digital/>
3. <https://www.simplilearn.com/introduction-to-cloud-computing-basics-skillup>
4. <https://www.geeksforgeeks.org/>
5. <https://www.javatpoint.com/>

CS-6623: MOBILE AND WIRELESS SYSTEMS

Course Outcomes (COs):

- CO1:** Learn the basic concepts of wireless and mobile technologies including; Mobile radio propagation, fading, diversity concepts and the channel modeling.
- CO2:** Discuss the cellular system design, implementation and technical challenges.
- CO3:** Understand satellite communication systems.
- CO4:** Know the features, applications, models and characteristics of adhoc and wireless sensor networks.
- CO5:** Understand the Wireless LAN and PAN architectures, protocols and expose students to emerging wireless technologies and their potential impact.
-

Course Contents

UNIT-I

No. of Hours: 8

Overview of the emerging field of mobile computing: Historical perspectives (mainly from the perspective of radio), Land mobile vs. Satellite vs. In-building communications systems, RF vs. IR, Mobile applications, Limitations, Health Concerns.

Mobile Radio Propagation: Introduction, Propagation mechanism, Path loss, Slow Fading, Fast Fading, Delay Spread, Inter-symbol Interference, Co-channel Interference.

UNIT-II

No. of Hours: 8

Cellular Concept: Characteristic of Cellular Systems, Cell area, Capacity of a cell, frequency reuse, Reducing Co-channel Interference, Cell Splitting, Cell Sectoring.

Mobile communication: Fiber or wire based transmission, Wireless Transmission: Frequencies, Antennas and Signal Propagation, Modulation Techniques, Multiplexing techniques, Coding techniques.

UNIT-III

No. of Hours: 8

Channel Allocation: Fixed Channel Allocation, Dynamic channel Allocation, Hybrid Channel Allocation, Allocation in Specialized System Structure.

Mobile Communication Systems: Cellular System Infrastructure, Registration, Handoff in cellular Systems, Roaming support, Mobile IP, Multicasting, Security and Privacy, Generation of Mobile Systems, Existing Wireless Systems, Case Study on GSM and CDMA.

UNIT-IV

No. of Hours: 8

Satellite Systems: Types of Satellite Systems, Characteristic of Satellite Systems, Satellite System Infrastructure, Call Setup, Global Positioning System, limitations and beneficiaries of GPS.

Ad Hoc and Sensor Networks: Characteristic of MANETs, Application, Routing, Routing Classification, Wireless Sensor Networks.

UNIT-V**No. of Hours: 8**

Wireless LANs and PANs: IEEE802.11, HIPERLAN, Bluetooth. Case Study on Wireless LAN infrastructure.

Mobile operating System, file system, Process, Task, Thread, ISR and IST, CODA, HTTP versus HTML, WML, XML application for wireless handheld devices.

UWB systems Characteristics, Signal propagations, technology, Mobility management for integrated systems, Current approaches for security.

Text Books:

1. Jochen Schiller, Mobile Communications, Pearson Education, 2nd Edition, 2008.
2. D. P. Agrawal and Qing-An zeng, Introduction to Wireless and Mobile Systems, Cengage India Private Limited; 3rd Edition, 2012.
3. P. Nicopotidis, M.S. Obaidat, G.I. Papadimitriou, and A.S. Pomportsis, Wireless Networks, Wiley publication, 2009.

Reference Books:

1. Raj Kamal, Mobile Computing, Oxford University press, 2007.
2. U. Hansmann, L. Merk, M.S. Nicklons and T. Stober, Principles of Mobile Computing, Springer, 2003.
3. R. Behravanfar, Mobile Computing Principles—Designing and Developing Mobile Applications with UML and XML, Cambridge University Press, 2005.
4. Andrew S. Tanenbaum, Computer Networks, Pearson Education, 4th Edition, 2003.
5. James F. Kurose and Keith W. Rose, Computer Networking, Pearson Education, 3rd Edition, 2005.

Online Resources:

1. NPTEL: Introduction to Wireless and Cellular Communications, available at: <https://archive.nptel.ac.in/courses/108/106/106106167/>
2. NPTEL: Wireless Communication, IIT Delhi By Prof. Ranjan Bose, available at: <https://nptel.ac.in/courses/117102062>
3. SWAYAM: Android Mobile Application Development, available at: https://onlinecourses.swayam2.ac.in/nou22_ge57/preview
4. Coursera: Wireless Communications for Everybody, available at: <https://www.coursera.org/learn/wireless-communications>
5. Computer Science 323: Wireless & Mobile Networking, available at: <https://study.com/academy/course/computer-science-323-wireless-mobile-networking.html>

CS-6623: MOBILE AND WIRELESS SYSTEMS - PRACTICAL

Course Outcomes (COs):

CO1: To Understand the android software stack / android architecture and the setting up the android development environment.

CO2: To develop android applications to create user Interfaces with basic controls, layouts and event driven controls

CO3: To develop android applications that make use of database, make use of notification manager, implements multithreading.

CO4: To develop android applications to demonstrate telephony operations.

CO5: To develop and a mobile application by preparing projects using Android.

Course Contents

UNIT-I

No. of Hours: 4

1. Understanding the Android Software Stack.
2. Installing the Android Studio and Android SDK.
3. Creating Android Virtual Devices.
4. Creating the First Android Project.
5. Understanding the Role of Android Application Components.
6. Understanding the Utility of Android API.
7. Knowing the Android Project Files.
8. Understanding Activities.
9. Understanding role of the Android Manifest File.

UNIT-II

No. of Hours: 4

1. Develop an application that uses GUI components, Font and Colours
2. Develop an application that uses Layout Managers and event listeners.
3. Develop an application to play audio and video of user's choice.
4. Write an application that draws basic graphical primitives on the screen.
5. Develop a native application that uses GPS location information

UNIT-III

No. of Hours: 4

1. Develop an application that makes use of databases.
2. Develop an application that makes use of Notification Manager.
3. Implement an application that uses Multi-threading.
4. Implement an application that writes data to the SD card.

UNIT-IV

No. of Hours: 4

1. Implement an application that creates an alert upon receiving a message
2. Write a mobile application that makes use of RSS feed

3. Develop a mobile application to send an email.

UNIT-V

No. of Hours: 4

Develop a Mobile application for simple needs (Mini Project)

Text Books:

1. Joseph Anuzzi, Lauren Darcey, and Shane Conder, "Introduction to Android Application Development: Android Essentials", 5th edition, Addison-Wesley Professional, 2015.

Reference Books:

1. Dr. John T Mesia Dhas, Dr. S. Naveen Kumar, and D. Surendra, "Android Applications Development Practical Approach", The Palm Series, Self-published by Dr. John T Mesia Dhas, 2021.

Online Resources:

1. SWAYAM: Android Mobile Application Development, available at: https://onlinecourses.swayam2.ac.in/nou22_ge57/preview
2. Android Developer guides, available at: <https://developer.android.com/guide>
3. Learn Android Application Development, available at: <https://www.udemy.com/course/learn-android-application-development-y/?srsltid=AfmBOorRO16WMMLe1K2yvHdeTFtq5c-46xaPD4B-ii7waVry9P65MhUP>