RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE FlexibleCurricula

CSE-Cyber Security/ Cyber Security,VII-Semester

CY-701-Machine Learning

COURSE OUTCOMES: After Completing the course student should be able to:

1. Apply knowledge of computing and mathematics to machine learning problems, models and algorithms.
2. Analyze a problem and identify the computing requirements appropriate for its solution.
3. Design, implement, and evaluate an algorithm to meet desired needs.
4. Apply mathematical foundations, algorithmic principles, and computer science theory to the modeling and design of computer-based systems in a way that demonstrates comprehension of the trade-offs involved in design choices.

Course Contents:

Unit –I
Introduction to machine learning, scope and limitations, regression, probability, statistics and linear algebra for machine learning, convex optimization, data visualization, hypothesis function and testing, data distributions, data preprocessing, data augmentation, normalizing data sets, machine learning models, supervised and unsupervised learning.

Unit –II
Linearity vs non linearity, activation functions like sigmoid, ReLU, etc., weights and bias, loss function, gradient descent, multilayer network, back propagation, weight initialization, training, testing, unstable gradient problem, auto encoders, batch normalization, dropout, L1 and L2 regularization, momentum, tuning hyper parameters**.**

Unit –III
Convolutional neural network, flattening, subsampling, padding, stride, convolution layer, pooling layer, loss layer, dance layer 1x1 convolution, inception network, input channels, transfer learning, one shot learning, dimension reductions, implementation of CNN like tensor flow, keras etc.

Unit –IV
Recurrent neural network, Long short-term memory, gated recurrent unit, translation, beam search and width, Bleu score, attention model, Reinforcement Learning, RL-framework, MDP, Bellman equations, Value Iteration and Policy Iteration, , Actor-critic model, Q-learning, SARSA.

Unit –V
Support Vector Machines, Bayesian learning, application of machine learning in computer vision, speech processing, natural language processing etc, Case Study: ImageNet Competition.

Recommended Books with Full Specification:

TEXT BOOKS:

1. Christopher M. Bishop, “Pattern Recognition and Machine Learning”, Springer-VerlagNew York Inc., 2nd Edition, 2011.
2. Tom M. Mitchell, “Machine Learning”, McGraw Hill Education, First edition, 2017.
3. Ian Goodfellow and Yoshua Bengio and Aaron Courville, “Deep Learning”, MIT Press,2016

REFERENCES:

1. Aurelien Geon, “Hands-On Machine Learning with Scikit-Learn and Tensorflow:Concepts, Tools, and Techniques to Build Intelligent Systems”, Shroff/O'Reilly; Firstedition (2017).
2. Francois Chollet, "Deep Learning with Python", Manning Publications, 1 edition (10January 2018).
3. Andreas Muller, "Introduction to Machine Learning with Python: A Guide for DataScientists", Shroff/O'Reilly; First edition (2016).
4. Russell, S. and Norvig, N. “Artificial Intelligence: A Modern Approach”, Prentice HallSeries in Artificial Intelligence. 2003

Practical’s:

Different problems to be framed to enable students to understand the concept learnt and get handsonon various tools and software related to the subject. Such assignments are to be framed for ten to twelve lab sessions.

RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE FlexibleCurricula

CSE-Cyber Security/ Cyber Security,VII-Semester

CY-702 (A) Penetration Testing and Vulnerability Analysis

Course Outcome: This course introduces students to the fundamentals of penetration testing and vulnerability analysis. Students will learn about the methods, tools, and techniques used to identify and exploit security vulnerabilities in computer systems, networks, and applications. The course will emphasize hands-on practical exercises and real-world scenarios to enhance understanding and develop skills in the field.

UNIT: 1 Introduction to penetration testing, Legal and ethical considerations, Types of penetration testing, Penetration testing methodologies. Information Gathering and Scanning: Foot printing and reconnaissance techniques, Network scanning and enumeration, SINT (Open-source intelligence) gathering, Vulnerability scanning tools.

UNIT 2: Exploitation and Post-Exploitation: Exploiting system and network vulnerabilities, Privilege escalation techniques, post-exploitation activities, Maintaining access and pivoting Web Application, Security, Introduction to web application security, Common web application vulnerabilities, Web application penetration testing methodologies, Web vulnerability scanners and tools.

UNIT 3: Wireless Network Security: Wireless network security concepts, Wi-Fi vulnerabilities and attacks, Wireless penetration testing techniques, securing wireless networks Social Engineering and Physical Security: Introduction to social engineering, Techniques and tactics of social engineering, Physical security vulnerabilities and testing, Mitigating social engineering and physical security risks.

UNIT 4: Cryptography and Secure Communications: Basics of cryptography, Cryptographic algorithms and protocols, Encryption, decryption, and key management, secure communication channelsReporting and Remediation: Documentation and reporting of findings, Prioritizing and mitigating vulnerabilities, engaging stakeholders and communicating recommendations, post-testing activities and continuous improvement.

UNIT 5: Mobile application security, Cloud security and testing (Internet of Things) security, red teaming and adversary simulation, Review of real-world penetration testing cases, Practical hands-on exercises, Capture the Flag (CTF) competitions, Final project and presentations.

Text Books:

1. Dafydd Stuttard and Marcus Pinto, "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws", Wiley Publication Year: 2011 (2nd edition).
2. David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni., “Metasploit: The Penetration Tester's Guide".
3. Patrick Engebretson, “The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy".

4. Michal Zalewski, “The Tangled Web: A Guide to Securing Modern Web Applications".
5. Mark Dowd, John McDonald, and Justin Schuh, “The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities".

Proposed List of Experiments:

1. Learn how to use tools like Nmap, Nessus, or OpenVAS to perform network scans and identify open ports, services, and potential vulnerabilities.
2. Implement Practice scanning a target network and analysing the results to identify potential attack vectors.
3. Implement Set up a vulnerable web application (e.g., OWASP Juice Shop or Damn Vulnerable Web Application) and practice identifying and exploiting security flaws.
4. Understand wireless network security concepts such as WEP, WPA, and WPA2 encryption.
5. Practice writing comprehensive penetration testing reports that highlight identified vulnerabilities, their impact, and recommended remediation steps.

RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE FlexibleCurricula

CSE-Cyber Security/ Cyber Security,VII-Semester

CY- 702(B) - Block Chain & Crypto-Currencies

Course Outcomes: After completing the course student should be able to:

1. To understand the basics of Blockchain
2. To learn Different protocols and consensus algorithms in Blockchain
3. To learn the Blockchain implementation frameworks
4. To understand the Blockchain Applications
5. To experiment the Hyper ledger Fabric, Ethereum networks

Unit 1:

Basics of Blockchain: Introduction, Concept of Blockchain, Fundamentals of Blockchain, Characteristics of Blockchain, Consensus in Trust-Building Exercise, Public, Private, and Hybrid Block chains, Distributed Ledger Technologies, Architecture of Blockchain, Transactions, Chaining Blocks, Value Proposition of Blockchain, Permissioned Model of Blockchain.

Unit 2:

Hash Functions, Hashing, Message Authentication Code, Secure Hash Algorithms (SHA-1), Distributed Hash Tables, Hashing in Blockchain Mining Consensus, Consensus Algorithm, Byzantine Agreement Methods.

Unit 3:

Blockchain Components, Ethereum Virtual Machine, Working of Ethereum, Ethereum Clients, Ethereum Transactions, , Ethereum Development Tools, Introduction of Cryptography, Cryptography Primitives, Symmetric Cryptography, Asymmetric Cryptography, Architecture of Hyper ledger.

Unit 4:

Smart Contracts, Absolute and Immutable, Contractual Confidentiality, Supply Chain Management, Darknet, The Future Bit coins, Working of Bitcoin, Merkle Trees, Bitcoin Block Structure, Bitcoin Address, Bitcoin Transactions Bitcoin Payments, Mining in Blockchain.

Unit 5:

Blockchain Vertical Solutions and Use Cases, Blockchain in Different domain like Insurance, Assets Management, healthcare etc., Smart Assets, Electronic Currency, Manufacturing Blockchain and Allied Technologies, Blockchain and Cloud Computing, Characteristics of Blockchain Cloud.

TEXT BOOKS

1. Blockchain Technology: Concepts and Applications by Kumar Saurabh, Ashutosh Saxena - John Wiley Publication.
2. Blockchain for Enterprise Application Developers by Ambadas Choudhari - John Wiley Publication
3. Bashir and Imran, Mastering Blockchain: Deeper insights into decentralization, cryptography, Bitcoin, and popular Blockchain frameworks, 2017.
4. Andreas Antonopoulos, “Mastering Bitcoin: Unlocking Digital Cryptocurrencies”, O’Reilly, 2014.

REFERENCE BOOKS

1. Daniel Drescher, “Blockchain Basics”, First Edition, Apress, 2017.
2. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press, 2016.
3. Melanie Swan, “Blockchain: Blueprint for a New Economy”, O’Reilly, 2015.
4. Ritesh Modi, “Solidity Programming Essentials: A Beginner’s Guide to Build Smart Contracts for Ethereum and Blockchain”, Packt Publishing.

5. Handbook of Research on Blockchain Technology published by Elsevier Inc. ISBN: 9780128198162, 2020.

List of Experiments:

1. Install and understand Docker container, Node.js, Java and Hyperledger Fabric, Ethereum and perform necessary software installation on local machine/create instance on cloud to run.
2. Create and deploy a blockchain network using Hyperledger Fabric SDK for Java Set up and initialize the channel, install and instantiate chain code, and perform invoke and query on your blockchain network.
3. Interact with a blockchain network. Execute transactions and requests against a blockchain network by creating an app to test the network and its rules.
4. Deploy an asset-transfer app using blockchain. Learn app development within a Hyperledger Fabric network.
5. Use blockchain to track fitness club rewards. Build a web app that uses Hyperledger Fabric to track and trace member rewards.

RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE FlexibleCurricula

CSE-Cyber Security/ Cyber Security,VII-Semester

CY- 702(C) -Mobile Security and Forensics

Pre-Requisite: Introduction to Digital Forensics.

Course Objectives

1. To gain knowledge on mobile phone evidence extraction process
2. To understand the practical mobile forensic approaches
3. To engage students in forensic acquisition and analysis of mobile computing devices, specifically Android device
4. To gain an understanding of mobile device identification

Course Outcomes:**After completing the course student should be able to:**

1. Understand what data is able to be acquire from mobile devices and be able to acquire and investigate data from mobile devices using forensically sound and industry standard tools.
2. Comprehend the relationship between mobile and desktop devices in relationship to criminal and corporate investigations.
3. Analyse mobile devices, their backup files, and artifacts for forensic evidence.

Course Contents:

Unit1: Introduction to Mobile Forensics: Mobile forensics, Challenges in mobile forensics The mobile phone evidence extraction, Documenting and reporting phase, Presentation phase, Archiving phase, Practical mobile forensic approaches: Overview of mobile operating systems, Data acquisition methods, Examination and analysis of evidence stored on mobile phones.

Unit2. Android Forensics : Understanding Android, Android model, Android security- Secure kernel, Security-Enhanced Linux, Full Disk Encryption, Trusted Execution Environment, Android file system. Android Forensic Setup and Pre-Data Extraction Techniques, Android Data Extraction Techniques, Android Data Analysis and Recovery, Android data recovery, Android App Analysis, Malware, and Reverse Engineering: Analyzing Android apps; Reverse engineering. Android apps; extracting an APK file from an Android device; Android malware.

Unit3. **iOS Forensics**: Introducing iOS Application Security, Basics of iOS and application development, Developing your first iOS app, Running apps on iDevice, iOS MVC design, iOS security model, iOS secure boot chain, iOS application signing, iOS application.

Unit4. Android Security: Sandboxing and the permission model, Application signing, Android startup process, Setting up the development environment, Creating an Android virtual device, Useful utilities for Android Pentest, Android Debug Bridge, Burp Suite, APKTool.

Unit5. Traffic Analysis: Traffic Analysis for Android Devices, Android traffic interception. Ways to analyze Android traffic, Passive analysis, Active analysis, HTTPS Proxy interception.

Recommended Books with Full Specification:

1. Cyber Security by Nina Godbole - John Wiley Publication.
2. Digital Forensic by Dr. Nilakshi Jain - John Wiley Publication
3. Aditya Gupta, “Learning Pentesting for Android Devices”, Packt Pub Ltd; Illustrated edition, 2014.
4. SwaroopYermalkar, “Learning iOS Penetration Testing Paperback”, Packt Publishing, 2004.

Text Books:

1. RohitTamma, Oleg Skulkin, Heather Mahalik, SatishBommisetty**,** “Practical Mobile Forensics - Third Edition”, Packt Publishing, 2018.
2. Igor Mikhaylov and Oleg Skulkin, “"Mobile Forensics Cookbook", Packt Publishing Limited, 2017.

List of Experiments:

1. Setup of memory forensic environment and extract various artifacts from memory dump and analyze the memory dump, using different tools like Volatility, LiME, etc.
2. Windows artifact analysis using different forensic tools, which includes MRU, link file, USB analysis, Prefetch analysis, shell bag, web cache etc.,
3. Using APKTool to reverse an Android application, Auditing Android applications.
4. Perform the following on different Android Image files: • Using a custom recovery android image. • Using AFLogical to extract contacts, calls, and text messages. • Dumping application databases manually. • Logging the logcat and using backup to extract an application's data.
5. Developing your first iOS app and running apps on iDevice.

RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE FlexibleCurricula

CSE-Cyber Security/ Cyber Security,VII-Semester

CY- 702(D) -Multimedia Security & Forensics

Course Objective:

1. Introduce multimedia, its application areas, data encoding and compression techniques.
2. Develop understanding of Quality of Service and its constraints.
3. Understand synchronization concepts.
4. Discuss multimedia security attacks and defense techniques.
5. To introduce multimedia forensic concepts.

Course Outcome: Students who successfully complete this course will be able to:-

1. Demonstrate how quality of service can be ensured in multimedia applications.
2. Apply different synchronization techniques on multimedia.
3. Ensure security of multimedia applications.
4. Perform forensic on multimedia data.

Unit -1: Introduction: Multimedia Application Areas, Interdisciplinary Aspects of Multimedia, Multimedia Data Encoding, Concept of data compression in multimedia field.

Unit-2: Quality of Service & Operating System: Requirements and Constraints, Quality of Services Concept, Resource Management, Media Server Architecture, Storage Management, Services, Protocols, Layers.

Unit-3: Security in Multimedia Applications: Security attacks, Multimedia Encryption, Steganography, Digital image watermarking, Multimedia Authentications.

Unit-4: Multimedia Evidence Handling: Digital Forensics Laboratories in Operation, Standards and Best Practices in Digital and Multimedia Forensics, Digital Evidence Extraction, Multimedia File Carving.

Unit-5: Multimedia Device and Source Forensics: Forensic Camera Model Identification, Printer and Scanner Forensics, Microphone Forensics, Multimedia Content Forensics.

Reference Books/Text Books

1. Ralf Steinmetz, Klara Nahrstedt. Multimedia Systems, Springer International Edition
2. Ho, Anthony TS, and Shujun Li, eds. Handbook of digital forensics of multimedia data and devices. John Wiley & Sons, 2015.
3. John. F. Koegel Buford. Multimedia Systems. Pearson Education.
4. Digital Watermarking and Steganography by Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica.

RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE FlexibleCurricula

CSE-Cyber Security/Cyber Security,VII-Semester

CY-703(A) -Ethical Hacking

Course Objectives:

1. The aim of the course is to introduce the methodologies framework tools of ethical hacking to get awareness in enhancing the security.
2 .To gain knowledge about Ethical hacking and penetration testing.
3. To learn about various types of attacks, attackers and security threats and vulnerabilities present in the computer system.
4. To examine how social engineering can be done by attacker to gain access of useful & sensitive information about the confidential data.
5. To gain knowledge of the tools, techniques and ethical issues likely to face the domain of ethical hacking and ethical responsibilities.

Course Outcomes:**After completing the course student should be able to:**

1. Describe and understand the basics of the ethical hacking and Gain the knowledge of the use and availability of tools to support an ethical hack.
2. Gain the knowledge of interpreting the results of a controlled attack.
3. Understand the role of politics, inherent and imposed limitations and metrics forplanning of a test.
4. Perform the foot printing and scanning.
5. Demonstrate the techniques for system hacking and Detect and prevent the security attacks in different environments.

Unit-I Ethical Hacking: Introduction, Networking & Basics, Foot printing and scanning: Information Gathering, Determining the Network Range, Identifying Active Machines, Finding Open Ports and Access Points, OS Fingerprinting Services, Mapping the Network Attack Surface. Google Hacking, Scanning, Windows Hacking, Linux Hacking.

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

Unit-III: Preparing for a Hack: Technical Preparation, Managing the Engagement Reconnaissance: Social Engineering, Physical Security, Internet Reconnaissance, Steganography, Cryptography, Wireless Hacking, Firewall & Honeypots, IDS & IPS, Vulnerability, Penetration Testing.

Unit–IV: Enumeration: Enumeration Techniques, Soft Objective, Looking Around or Attack, Elements of Enumeration, Preparing for the Next Phase Exploitation: Intuitive Testing, Evasion, Threads and Groups, Operating Systems, Password Crackers, RootKits, applications, Wardialing, Network, ServicesDoS attacks and Areas of Concern.

Unit-V: Reverse Engineering, Email Hacking, Incident Handling & Response, Bluetooth Hacking, Mobile Phone Hacking Basic ethical hacking tools and usage of these tools in a professional environment. Legal, professional and ethical issues likely to face the domain of ethical hacking. Ethical responsibilities, professional integrity and making appropriate use of the tools and techniques associated with ethical hacking.

Text Books

1. James S. Tiller, “The Ethical Hack: A Framework for Business Value Penetration Testing”, Auerbach Publications, CRC Press
2. EC-Council, “Ethical Hacking and Countermeasures Attack Phases”, Cengage Learning
3. Michael Simpson, Kent Backman, James Corley, “Hands-On Ethical Hacking and Network Defense”, Cengage Learning.
4. Hacking For Dummies, 6ed by Kevin Beaver - John Wiley Publication

5. Digital Forensic by Dr. Nilakshi Jain - John Wiley Publication

References:

1. Certified Ethical Hacker, Version 9, Second Edition, Michael Gregg, Pearson IT Certification.
2. Hacking the Hacker, Roger Grimes, Wiley.
3. The Unofficial Guide to Ethical Hacking, AnkitFadia, Premier Press.

List of Experiments :--(Ethical Hacking Lab)

1. List the tools for Ethical Hacking.
2. Implement Foot-printing and Reconnaissance using tools.
3. Setup a honey pot and monitor the honey pot on network.
4. Create a social networking website login page using phishing techniques.
5. Write a code to demonstrate DoSattacks.
6. Install rootkits and study variety of options.
7. Study of Techniques uses for Web Based Password Capturing.
8. Implement passive scanning, active scanning, session hijacking, cookies extraction using Burp suit tool.

RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE FlexibleCurricula

CSE-Cyber Security/ Cyber Security,VII-Semester

CY-703(B) -Cyber Security Policies & Standards

The objective of the courses to
1) Understand the fundamental s of cyber security and cyber crimes.
2) Understand the tools and methods in cybercrimes and understanding computer forensics.

Course Outcomes:**After completing the course student should be able to:**

1. Analyze cyber-attacks, types of cybercrimes, cyber laws and also how to protect them self and ultimately the entire Internet community from such attacks.
2. Interpret and forensically investigate security incidents.
3. Apply security policies and procedures to manage Privacy issues and cyber laws.
4. Design and develop secure software modules.

Course Contents:

Unit 1
Introduction to Cyber Security: Basic Cyber Security Concepts, layers of security, Vulnerability, threat, Harmful acts, Internet Governance – Challenges and Constraints, Computer Criminals, CIA Triad, Assets and Threat, motive of attackers, active attacks, passive attacks, Software attacks, hardware attacks, Cyber Threats-Cyber Warfare, Cyber Crime, Cyber terrorism, Cyber Espionage, etc., Comprehensive Cyber Security Policy.

Unit 2
Cyberspace and the Law & Cyber Forensics: Introduction, Cyber Security Regulations, Roles of International Law. The INDIAN Cyberspace, National Cyber Security Policy. Introduction, Historical background of Cyber forensics, Digital Forensics Science, The Need for Computer Forensics, Cyber Forensics and Digital evidence, Forensics Analysis of Email, Digital Forensics Lifecycle, Forensics Investigation, Challenges in Computer Forensics.

Unit3
Organizational Implications ofCyber Security: Introduction cost of cybercrimes and IPR issues, web threats for organizations, security and privacy implications, social media marketing: security risks and perils for organizations, social computing and the associated challenges for organizations.

Unit4
Privacy Issues: Basic Data Privacy Concepts: Fundamental Concepts, Data Privacy Attacks, Datalinking and profiling, privacy policies and their specifications, privacy policy languages, privacy in different domains- medical, financial etc.

Unit5
Introduction to security policies and cyber laws:-Need for An Information Security Policy, Information Security Standards – ISO, Introducing Various Security Policies and Their Review Process, Introduction to Indian Cyber Law, Objective and Scope of the IT Act, 2000, Intellectual Property Issues, Overview of Intellectual Property Related Legislation in India, Patent, Copyright, Law Related to Semiconductor Layout and Design, Software License.

Recommended Books with Full Specification:

TEXT BOOKS:

1. Nina Godbole and SunitBelpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley

2. B.B.Gupta,D.P.Agrawal,HaoxiangWang, Computer andCyberSecurity:Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335, 2018.

3. Dr. Surya PrakashTripathi, RitendraGoyal, Praveen Kumar Shukla, KLSI. “Introduction to information security and cyber laws”. Dreamtech Press. ISBN: 9789351194736, 2015.

4. Cyber Security and Cyber Laws by Dr. Nilakshi Jain - John Wiley Publication.

5. Digital Forensic by Dr. Nilakshi Jain - John Wiley Publication.

REFERENCES:

1. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRCPress.

2. Introduction to Cyber Security, Chwan-Hwa (john) Wu,J. David Irwin, CRC Press T&FGroup.

List of Experiments:

1. Cybercrime: Examples and Mini-Cases (Case Study)
2. Examples: Official Website of Maharashtra Government Hacked, Indian Banks Lose Millions of Rupees, Parliament Attack, Pune City Police Bust Nigerian Racket, e-mail spoofing instances.
3. Mini-Cases: The Indian Case of online Gambling, An Indian Case of Intellectual Property Crime, Financial Frauds in Cyber Domain.

RAJIV GANDHI PROUDHOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE-Cyber Security /Cyber Security, VII Semester

CY-703 (C) Data Engineering

UNIT 1: Introduction to Data Engineering: Definition, Evolution, Life Cycle, Data Engineering skills and activities, Data Maturity, Data Lifecycle Versus the Data Engineering Lifecycle, Security, Data Management, DataOps.

UNIT 2: Source Systems and Data Ingestion: Types of Data Architecture, Data Lake,Data Lakehouses,Modern Data Stack, Lambda Architecture, Kappa Architecture.

UNIT 3: Data Platforms, Stream-to-Batch Storage Architecture, Data Catalog, Data Sharing,Data Modeling,Dimensional Modeling,Creating Tables,Schema Migration,Building the data warehouse.

UNIT 4: Data Ingestion, SFTP and SCP, Webhooks, Web Interface, Web Scraping Business Intelligence Tools,Introduction to Superset,Creating visualizations,Data Quality, Data Catalogs, Data Lineage, and Data Governance.

UNIT 5: ETL, Reverse ETL, Security, Privacy, and the Future of Data Engineering, Patch and Update Systems, Logging, Monitoring, and Alerting.

Recommended Books with Full Specification:

1. Fundamentals of Data Engineering by Joe Reis, Matt Housley Released June 2022, and Publisher: O'Reilly Media, Inc. NISBN: 9781098108304.
2. Data Engineering with Python: Work with Massive Datasets to Design Data Models and Automate Data Pipelines Using Python by Paul Crickard.

RAJIV GANDHI PROUDHOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE-Cyber Security /Cyber Security, VII Semester

CY-703 (D) Cloud Computing

Course Objective: The objective of this course is to provide students with the comprehensive and indepth knowledge of Cloud Computing concepts, technologies, architecture and applications.

Course Outcomes: After the completion of this course, the students will be able to:

1. Explain the core concepts of the cloud computing paradigm
2. Demonstrate knowledge of virtualization
3. Explain the core issues of cloud computing such as security, privacy, and interoperability.
4. Choose the appropriate technologies, algorithms, and approaches for the related issues.
5. Identify problems, and explain, analyze, and evaluate various cloud computing solutions

UNIT I: Introduction of Grid and Cloud computing, characteristics, components, business and ITperspective, cloud services requirements, cloud models, Security in public model, public verses private clouds, Cloud computing platforms: Amazon EC2,Platform as Service: Google App Engine, Microsoft Azure, Utility Computing, Elastic Computing.

UNIT II: Cloud services- SAAS, PAAS, IAAS, cloud design and implementation using SOA, conceptual cloud model, cloud stack, computing on demand, Information life cycle management, cloud analytics, information security, virtual desktop infrastructure, storage cloud.

UNIT III: Virtualization technology: Definition, benefits, sensor virtualization, HVM, study of hypervisor, logical partitioning- LPAR, Storage virtualization, SAN, NAS, cloud server virtualization, virtualized data center.

UNIT IV: Cloud security fundamentals, Vulnerability assessment tool for cloud, Privacy and Security in cloud, Cloud computing security architecture: Architectural Considerations- General Issues, Trusted Cloud computing, Secure Execution Environments and Communications, Micro- architectures; Identity Management and Access control-Identity management, Access control, Autonomic Security, Cloud computing security challenges: Virtualization security management- virtual threats, VM Security Recommendations, VM-Specific Security techniques, Secure Execution Environments and Communications in cloud.

UNIT V: SOA and cloud, SOA and IAAS, cloud infrastructure benchmarks, OLAP, business intelligence, e-Business, ISV, Cloud performance monitoring commands, issues in cloud computing. QOS issues in cloud, mobile cloud computing, Inter cloud issues, Sky computing, Cloud Computing Platform, Xen Cloud Platform, Eucalyptus, OpenNebula, Nimbus, TPlatform, Apache Virtual Computing Lab (VCL), Anomaly Elastic Computing Platform.

Recommended Books with Full Specification:

1. Dr.Kumar Saurabh, “Cloud Computing”, Wiley India.
2. Ronald Krutz and Russell Dean Vines, “Cloud Security”, Wiley-India.
3. Judith Hurwitz, R.Bloor, M.Kanfman, F.Halper, “Computing for Dummies”, Wiley India Edition.
4. Anthony T.Velte Toby J.Velte, “Cloud Computing – A Practical Approach”, TMH.
5. Barrie Sosinsky, ‘Cloud Computing Bible”, Wiley India.