

RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE Internet of Things and Cyber Security Including Block Chain Technology, V-Semester

IS 501- FOUNDATIONS OF BLOCKCHAIN TECHNOLOGY

UNIT-I

Introduction to Blockchain:Need for Distributed Record Keeping,Blockchain architecture, blockheader detailed design, Abstract Models for Blockchain, Proof of Work (PoW), liveness and fairness, Proof of Stake (PoS) based Chains, Hybrid models (PoW + PoS); Types of Blockchain..

UNIT-II

Blockchain Consensus Algorithm challenges and solutions,Modeling faults and adversaries,Byzantine Models of Fault tolerance;Zero Knowledge proofs and protocols in Blockchain.

UNIT-III

Introduction to cryptographic basics for cryptocurrency - a short description of Hashing, digital signature schemes, encryption schemes and elliptic curve cryptography, verifiable random functions.

UNIT-IV

Blockchain 2.0: Introduction to Ethereum, Ethereum Virtual Machine (EVM), Wallets for Ethereum, Solidity, Smart Contracts, Attacks on smart contracts, The Turing Completeness of Smart Contract Languages and verification challenges. Blockchain 3.0: Hyperledger implementation on Ethereum,the plug and play platform and mechanisms in permissioned blockchain.

UNIT-V

Application of Blockchain:Bitcoin- Bitcoin consensus, Wallet, Bitcoin Blocks, Merkley Tree, hardness of mining, transaction verifiability, anonymity, forks, double spending, mathematical analysis of properties of Bitcoin. Altcoins. Medical record management systems, DNS records.

BOOKS RECOMMENDED:

1. Josh Thompson, 'Blockchain: The Blockchain for Beginnings, Guide to Blockchain Technology and Blockchain Programming', Create Space Independent Publishing Platform, 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. Kumar Saurabh, AshutoshSaxena, 'Blockchain Technology: Concepts and Applications', Wiley, 2020.

RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE Internet of Things and Cyber Security Including Block Chain Technology, V-Semester

IS 502- Database Management Systems

COURSE OBJECTIVES: The objective of this course is to enable students in developing a high level understanding of the concepts of Database management systems in contrast with traditional data management systems with emphasis on skills to apply these concepts in building, maintaining and retrieving data from these DBMS.

COURSE OUTCOMES:

After completing the course student should be able to:

1. Describe design of a database at various levels and compare and contrast traditional data processing with DBMS.
2. Design a database using Entity Relationship diagram and other design techniques.
3. Apply fundamentals of relational model to model and implement a sample Database Management System for a given domain.
4. Evaluate and optimize queries and apply concepts of transaction management.

COURSE CONTENTS:

UNIT I: DBMS Concepts and architecture Introduction, Database approach v/s Traditional file accessing approach, Advantages of database systems, Data models, Schemas and instances, Data independence, Data Base Language and interfaces, Overall Database Structure, Functions of DBA and designer, ER data model: Entities and attributes, Entity types, Defining the E-R diagram, Concept of Generalization, Aggregation and Specialization. Transforming ER diagram into the tables. Various other data models object oriented data Model, Network data model, and Relational data model, Comparison between the three types of models. Storage structures: Secondary Storage Devices, Hashing & Indexing structures: Single level & multilevel indices.

UNIT II: Relational Data models: Domains, Tuples, Attributes, Relations, Characteristics of relations, Keys, Key attributes of relation, Relational database, Schemas, Integrity constraints. Referential integrity, Intension and Extension, Relational Query languages: SQL-DDL, DML, integrity constraints, Complex queries, various joins, indexing, triggers, assertions, Relational algebra and relational calculus, Relational algebra operations like select, Project, Join, Division, outer union. Types of relational calculus i.e. Tuple oriented and domain oriented relational calculus and its operations.

UNIT III: Data Base Design: Introduction to normalization, Normal forms- 1NF, 2NF, 3NF and BCNF, Functional dependency, Decomposition, Dependency preservation and lossless join, problems with null valued and dangling tuples, multivalued dependencies. Query Optimization: Introduction, steps

of optimization, various algorithms to implement select, project and join operations of relational algebra, optimization methods: heuristic based, cost estimation based.

UNIT IV: Transaction Processing Concepts: -Transaction System, Testing of Serializability, Serializability of schedules, conflict & view serializable schedule, recoverability, Recovery from transaction failures. Log based recovery. Checkpoints deadlock handling. Concurrency Control Techniques: Concurrency Control, locking Techniques for concurrency control, time stamping protocols for concurrency control, validation based protocol, multiple granularity. Multi version schemes, Recovery with concurrent transaction. Introduction to Distributed databases, data mining, data warehousing, Object Technology and DBMS, Comparative study of OODBMS Vs DBMS . Temporal, Deductive, Multimedia, Web & Mobile database.

UNIT V: Case Study of Relational Database Management Systems through Oracle/PostgreSQL/MySQL: Architecture, physical files, memory structures, background process. Data dictionary, dynamic performance view. Security, role management, privilege management, profiles, invoker defined security model. SQL queries, Hierarchical queries, inline queries, flashback queries. Introduction of ANSI SQL, Cursor management: nested and parameterized cursors. Stored procedures, usage of parameters in procedures. User defined functions their limitations. Triggers, mutating errors, instead of triggers.

TEXT BOOKS RECOMMENDED:

1. Korth H.F. &Silberschatz A., Sudarshan, “Database Systems”, McGraw-Hill
2. Chris J. Date, with Hugh Darwin, Addison-Wesley, “A Guide to SQL Standard”.
3. Elmasri R., Navathe S.B., “Fundamentals of Database Systems”, Pearson.

REFERENCE BOOKS:

1. Rob, “ Database System: Design Implementation & Management”, Cengage Learning.
2. AtulKahate , “Introduction to Database Management System”, Pearson Educations
3. Oracle 9i Database Administration Fundamental-I, Volume I, Oracle Press, TMH.
4. Paneerselvam,”Database Management System”, PHI Learning

RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE Internet of Things and Cyber Security Including Block Chain Technology, V-Semester

IS 503 (A) Security Assessment and Risk Analysis

Course Outcomes: After completion of course, students would be able:

1. To apply contingency strategies including data backup and recovery and alternate site selection for business resumption planning
2. To Skilled to be able to describe the escalation process from incident to disaster in case of security disaster.
3. To Design a Disaster Recovery Plan for sustained organizational operations.

Course Objective:

Describe the concepts of risk management in information security Define and differentiate various Contingency Planning components. Define and be able to discuss incident response options, and design an Incident Response Plan for sustained organizational operations.

Course Contents:

Unit I :

SECURITY BASICS: Information Security (INFOSEC) Overview: critical information characteristics – availability information states – processing security countermeasures-education, training and awareness, critical information characteristics – confidentiality critical information characteristics – integrity, information states – storage, information states – transmission, security countermeasurespolicy, procedures and practices, threats, vulnerabilities.

Unit II :

Threats to and Vulnerabilities of Systems: Threats, major categories of threats (e.g., fraud, Hostile Intelligence Service (HOIS). Countermeasures: assessments (e.g., surveys, inspections). Concepts of Risk Management: consequences (e.g., corrective action, risk assessment), cost/benefit analysis and implementation of controls, monitoring the efficiency and effectiveness of controls (e.g., unauthorized or inadvertent disclosure of information).

Unit III :

Security Planning: directives and procedures for policy mechanism. Contingency Planning/Disaster Recovery: agency response procedures and continuity of operations, contingency plan components, determination of backup requirements, development of plans for recovery actions after a disruptive event.

Unit IV :

Personnel Security Practices and Procedures: access authorization/verification (need- to-know), contractors, employee clearances, position sensitivity, security training and awareness, systems

maintenance personnel.

Auditing and Monitoring: conducting security reviews, effectiveness of security programs, investigation of security breaches, privacy review of accountability controls, review of audit trails and logs.

Unit V :

Operations Security (OPSEC): OPSEC surveys/OPSEC planning INFOSEC: computer security – audit, cryptography-encryption (e.g., point-to-point, network, link). Case study of threat and vulnerability assessment.

Text Books/References:

1. Information Systems Security, 2ed: Security Management, Metrics, Frameworks and Best Practices, Nina Godbole, John Wiley & Sons.
2. Principles of Incident Response and Disaster Recovery, Whitman & Mattord, Course Technology ISBN: 141883663X.

Corresponding Online Resources:

1. Introduction to Cyber Security, https://swayam.gov.in/nd2_nou20_cs01/preview
2. (Web Link) http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf

RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE Internet of Things and Cyber Security Including Block Chain Technology, V-Semester

IS 503 (B) Software Engineering

Unit I : The Software Product and Software Process

Software Product and Process Characteristics, Software Process Models: Linear Sequential Model, Prototyping Model, RAD Model, Evolutionary Process Models like Incremental Model, Spiral Model, Component Assembly Model, RUP and Agile processes. Software Process customization and improvement, CMM, Product and Process Metrics

Unit II : Requirement Elicitation, Analysis, and Specification

Functional and Non-functional requirements, Requirement Sources and Elicitation Techniques, Analysis Modeling for Function-oriented and Object-oriented software development, Use case Modeling, System and Software Requirement Specifications, Requirement Validation, Traceability

Unit III : Software Design

The Software Design Process, Design Concepts and Principles, Software Modeling and UML, Architectural Design, Architectural Views and Styles, User Interface Design, Function- oriented Design, SA/SD Component Based Design, Design Metrics.

Unit IV : Software Analysis and Testing

Software Static and Dynamic analysis, Code inspections, Software Testing, Fundamentals, Software Test Process, Testing Levels, Test Criteria, Test Case Design, Test Oracles, Test Techniques, Black-Box Testing, White-Box Unit Testing and Unit, Testing Frameworks, Integration Testing, System Testing and other Specialized, Testing, Test Plan, Test Metrics, Testing Tools. , Introduction to Object-oriented analysis, design and comparison with structured Software Engg.

Unit V : Software Maintenance & Software Project Measurement

Need and Types of Maintenance, Software Configuration Management (SCM), Software Change Management, Version Control, Change control and Reporting, Program Comprehension Techniques, Re-engineering, Reverse Engineering, Tool Support. Project Management Concepts, Feasibility Analysis, Project and Process Planning, Resources Allocations, Software efforts, Schedule, and Cost estimations, Project Scheduling and Tracking, Risk Assessment and Mitigation, Software Quality Assurance (SQA). Project Plan, Project Metrics.

Books Recommended:

1. Pressman R.S., “Software Engineering – A Practitioners Approach”, McGraw Hill.
2. Sommerville, “Software Engineering”, Pearson Education
3. Pankaj Jalote, “An Integrated Approach to Software Engineering”, Narosa Publishing House.
4. Stephen Schach, “Software Engineering”, Tata McGraw Hill.
5. Waman S. Jawadekar, “Software Engineering – Principles and Practice”, McGraw Hill.
6. Stephen H. Kan, “Matrix and Models in Software Quality Engineering”, Addison Wesley.

RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE Internet of Things and Cyber Security Including Block Chain Technology, V-Semester

IS 503 (C) E-commerce Security

UNIT: 1 Introduction to E-commerce: Operating System Services, Advantages and Disadvantages of E – Commerce, Developer Services, Data Services, Application Services, Store Services, Client Services, Types of E Commerce Solutions- Direct Marketing and Selling, Supply Chain Integration, Corporate Procurement.

UNIT: 2 Business Models for E-Commerce: E-Business models based on Relationship of Transaction Parties, Brokerage Model, Aggregator Model, Info-mediary model, Community Model, Value chain model, Manufacturer model, Advertising Model, Subscription model, E-Marketing – Identifying Web Presence Goals, Browsing Behaviour Model, Building Customer Relationship Based on One – to – One Marketing, E – branding, Elements of Branding, Spiral Branding.

UNIT:3 Electronic Data Interchange: Evolution, uses, Benefits, Working of EDI, EDI Standards (includes variable length EDI standards), Cost Benefit Analysis of EDI, Electronic Trading Networks, EDI Components, File Types, EDI Services, EDI Software, Business Approach of EDI, EDIFACT (Overview, Structure, EDIFACT Software), Business Future of EDI, EDI Administration. EDI Security, Digital signatures, Digital Certificates, Cryptography export restrictions, Secure Sockets Layer (SSL), Secure Electronic Transactions (SET), Smart Cards and its applications, WAP, WAP Architecture, WAP Programming Model.

UNIT: 4 Electronic Payment Security: Electronic Payment Systems – Electronic Commerce, Offline Versus Online, Debit Versus Credit, Macro versus Micro, Payment Instrument, Electronic Wallet, Smart Cards, Electronic Payment Security. Payment Security Services – Payment Transaction Security, Digital Money Security, Electronic Check Security, Availability and Reliability, Electronic Payment Framework.

UNIT: 5 Security on the Web & Mobile : Network and Website Security Risks, HTTP Cache Security Issues, HTTP Client Authentication, Web Transaction Security, Web Server Security, Web Client Security, Mobile Agent Security – mobile Agents, Security Issues, Protecting Platforms from Hostile Agents, Smart Card Security, Firewall Concept, Firewall Components, Benefits of an Internet Firewall, Enterprise-Wide Security Framework, Secure Physical Infrastructure.

References:

- 1) E-Commerce: Fundamentals and Applications, Henry Chan, Wiley India
- 2) E-Commerce An Indian Perspective, P.T. Joseph, S.J., PHI.
- 3) Electronic Commerce: Greenstein, Merylin, Tata Mc.Graw Hill.
- 4) E-Commerce Business Technology. Society, Kenneth C. Laudon, Carol Guerico Traver, Pearson Education.

RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE Internet of Things and Cyber Security Including Block Chain Technology, V-Semester

IS 504 (A) Cyber security Operations

Prerequisites :

CyberOps Associate students should have the following skills and knowledge:

- PC and internet navigation skills
- Basic Windows and Linux system concepts
- Basic understanding of computer networks
- Binary and Hexadecimal understanding

Course Outcome :

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

- Explain the role of the Cybersecurity Operations Analyst in the enterprise.
- Analyze the operation of network protocols and services.
- Explain the operation of the network infrastructure.
- Classify the various types of network attacks.
- Use network monitoring tools to identify attacks against network protocols and services.
- Evaluate network security alerts.
- Analyze network intrusion data to identify compromised hosts.

Unit I :

Cybersecurity incidents, Threat actors, network security attacks, security operations center, security features of the Windows & Linux operating systems, Linux file system and permissions.

Unit II :

Network Security Infrastructure : Network Topologies, Security Devices, Security Services, Network Attacks, types of attack tools used by Threat Actors. Network Monitoring and Tools.

Unit III :

TCP/IP vulnerabilities : IP PDU Details, TCP and UDP Vulnerabilities, IP service vulnerabilities, network security defense : Defense-in-Depth, Security Policies, Regulations, and Standards,

Unit IV :

Network Protection : Access Control Concepts, AAA usage and operation, Threat Intelligence : Information Sources, Threat Intelligence Services, Endpoint Protection : Antimalware Protection, Host-based Intrusion Prevention, Application Security.

Unit V :

Endpoint Vulnerability Assessment, Network and Server Profiling, Common Vulnerability Scoring System (CVSS), Information Security Management Systems, Network Security Data, Evaluating Alerts, Cyber Kill Chain, Diamond Model of Intrusion Analysis,

References :

1. Cybersecurity Operations Companion Guide by Cisco Networking Academy, Cisco Press 2018
2. Cybersecurity Operations Handbook by Bill Hancock, John W. Rittinghouse, and William M. Hancock, PhD, CISSP, CISM, Elsevier Science
3. Security Operations Center: Building, Operating, and Maintaining Your SOC by Gary McIntyre, Joseph Muniz, and Nadhem AlFardan, Cisco Press.

RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE Internet of Things and Cyber Security Including Block Chain Technology, V-Semester

IS 504 (B) Digital Forensic

Unit I :

Introduction to Digital Forensics, Physical Vs Cyber crime, Digital Vs Physical Evidence, Nature of Digital Evidence, Preservation of Digital Evidence, Challenging aspects of Digital Evidence, Digital Devices; Principles of Digital Forensics, Digital Forensic Investigation, Investigation Models.

Unit II :

Data and Evidence Recovery: Seizure of digital Evidence- Issues, methodology, factors limiting wholesale seizure, pulling the plug or not; Data objects, Storage Media, Variety of data, Recovered data objects, electronic evidence- secure boot and write blockers, disk file organization, disk and file imaging recovering techniques.

Unit III :

Mobile and Live Forensics Investigations: Mobile phone forensics- Mobile device characteristics, memory considerations, tools classification, flasher boxes, obstructed devices; Forensics procedures- preservation, acquisition, examination and analysis, reporting; SIM Card Forensics.

Unit IV:

Network Forensics: Sources of network based evidences, procedure for applying network based forensics, digital evidence on internet, digital evidence on physical and data link layers, digital evidence at the network and transport layers.

Unit V:

Case Study of Data recovery and Forensic tools: FTK, Encase, Mini tool, Win-LiFT, SIMXtractor etc., Memory dump tools like: winddumpt etc.

Books Recommended:

- [1] Ibrahim Baggili, Digital Forensics and Cyber Crime, Springer.
- [2] W. Kruse and J. Heiser, Computer Forensics: Incident Response Essentials, Massachusetts, Ed. Boston, Addison Wesley.
- [3] Rick Ayers, Sam Brothers and Wayne Jansen, Guidelines on Mobile Device Forensics, NIST, 2014.

RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE Internet of Things and Cyber Security Including Block Chain Technology, V-Semester

IS 504 (C) Cyber Law & Emerging Jurisprudence

UNIT: 1 Introduction: Defining Cyber Space, Cyber Law and IT Act 2000, Jurisdiction in Cyber Space, Contracts, Electronic Contracts, Cyber Contracts and Indian Legal Position.

UNIT: 2 Faith in Cyber World: Digital Signature and Electronic Signature, Electronic Governance, Internet Governance.

UNIT: 3 Cyber Crimes: Introduction to Cyber Crimes, Law Relating to Cyber Crimes, Procedural Law & Other Laws Relating to Cyber Crime, Evidence Act.

UNIT: 4 International Laws and Cyber Crimes: Cyber Crime in International Perspective.

UNIT: 5 Case Laws: Study of Landmark Cases relating to Cyber Crime (1) Hacking. (2) Obscenity & Pornography. (3) Cyber Stalking (4) Cyber Terrorism. (5) Identity Theft. (6) Cyber Fraud.

References:

- 1) The Indian Cyber law with Cyber glossary, Suresh T. Vishwanathan, New Delhi, Bhart Law House, 2000.
- 2) Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives, Nina Godbole, Sunit Belapure, Wiley India
- 3) Law of Cyber Crimes and Information Technology Law, S.V. JogaRao, 2007.
- 4) Cyber Law, Cyber Crime Internet and E-Commerce, Vimlendu Tayal.
- 5) Information Technology Law and Practice, Vakul Sharma.