IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VIII Semester

VIII Semester (Scheme-A)

Sr. No.	Course Type	Course Code	Course Title	Scheme			Credits
				L	T	P	
1	PEC	CB04	Professional Elective -IV	3	–	–	3
2	PEC	CB05	Professional Elective-V	3	–	–	3
3	SBC	CB03(P)	Penetration Testing and Vulnerability Analysis Lab	–	–	4	2
4	PROJ	CB06(A)	Project-III	–	–	16	8
Total Academic Engagement and Credits				**6**	–	**20**	**16**
				26			

VIII Semester (Scheme-B)

Sr. No.	Course Type	Course Code	Course Title	Scheme			Credits
				L	T	P	
1	PEC	CB04	Professional Elective -IV	3	–	–	3
2	PEC	CB05	Professional Elective-V	3	–	–	3
3	SBC	CB03(P)	Penetration Testing and Vulnerability Analysis Lab	–	–	4	2
4	PROJ	CB06(A)	Internship and Project (Industry/Corporate/Academia)	–	–	16	8
Total Academic Engagement and Credits				**6**	–	**20**	**16**
				26			

- Professional Elective–IV -

(A) Hardware Security
(B) Industry use cases using Block Chain
(C) Natural Language Processing
(D) Database Security

- Professional Elective–V

(A) Mobile and Wireless Security
(B) Knowledge Management
(C) Data Visualization
(D) Data Mining and Warehousing
(E) Information Systems & Infrastructure Security Management

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VIII Semester

PEC-CB04(A)	Hardware Security	3L:0T:0P (3hrs.)	3 Credits

Pre-requisite: NA

Course Objective: This course introduces the fundamentals of hardware security, covering cryptographic hardware design, FPGA implementation, and public key cryptography basics. It explores security primitives like PUFs, side-channel attacks and defenses, verification, fault tolerance, and methods to prevent hardware and IP piracy.

Course Contents: (40hrs)

Module 1: **(06hrs.)**
Overview of Different Issues of Hardware Security , Algebra of Finite Fields, Basics of the Mathematical Theory of Public Key Cryptography, Basics of Digital Design on Field-programmable Gate Array (FPGA), Classification using Support Vector Machines (SVMs).

Module 2: **(08hrs.)**
Useful Hardware Security Primitives: Cryptographic Hardware and their Implementation, Optimization of Cryptographic Hardware on FPGA, Physically Unclonable Functions (PUFs), PUF Implementations, PUF Quality Evaluation, Design Techniques to Increase PUF Response Quality.

Module 3: **(10hrs.)**
Side-channel Attacks on Cryptographic Hardware: Basic Idea, Current-measurement based Side-channel Attacks (Case Study: Kochers Attack on DES), Design Techniques to Prevent Sidechannel Attacks, Improved Side-channel Attack Algorithms (Template Attack, etc.), Cache Attacks

Module 4: **(08hrs.)**
Testability and Verification of Cryptographic Hardware: Fault-tolerance of Cryptographic Hardware, Fault Attacks, Verification of Finite-field Arithmetic Circuits, Modern IC Design and Manufacturing Practices and Their Implications.

Module 5: **(08hrs.)**
Hardware Intellectual Property (IP) Piracy and IC Piracy, Design Techniques to Prevent IP and IC Piracy, Using PUFs to prevent Hardware Piracy, Model Building Attacks on PUFs (Case Study: SVM Modelling of Arbiter PUFs, Genetic Programming based Modelling of Ring Oscillator PUF)

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)

Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VIII Semester

Course Outcome:

1. Understand and optimize the process of implementing cryptographic algorithms on hardware
2. Learn the different kinds of attacks that can be mounted against cryptographic algorithms
3. Learn the process of building Physical Unclonable Functions and make them resilient to attacks
4. Understand the different kinds of Trojans, their impact and learn the effective countermeasures for defending against them.
5. Learn the different kinds of threats at the micro architectural level and their corresponding Counter measures.

List of Text Book:

1. Debdeep Mukhopadhyay and RajatSubhra Chakraborty, "Hardware Security: Design, Threats, and Safeguards", CRC Press.
2. Ahmad-Reza Sadeghi and David Naccache (eds.): Towards Hardware-intrinsic Security: Theory and Practice, Springer.
3. Ted Huffmire et al: Handbook of FPGA Design Security, Springer.
4. Stefan Mangard, Elisabeth Oswald, Thomas Popp: Power analysis attacks - revealing the secrets of smart cards. Springer 2007.
5. Doug Stinson, Cryptography Theory and Practice, CRC Press.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VIII Semester

PEC-CB04(B)	**Industry use cases using Block Chain**	**3L:0T:0P (3hrs.)**	**3 Credits**

Pre-requisite:

Course Objective: This course provides a comprehensive introduction to blockchain technology, covering its architecture, cryptographic foundations, and consensus mechanisms. It also explores permissioned blockchains like Hyperledger Fabric, real-world industry applications, security frameworks, and emerging research areas including scalability, AI integration, and big data.

Course Contents: (40hrs)

Module 1: **(06hrs.)**
Introduction to Blockchain – I (Basics, History, Architecture, Conceptualization), Basic Crypto Primitives, Distributed Consensus, Consensus in Bitcoin – I (The Basics, PoW and Beyond, The Miners), Permissioned Blockchain (Basics, Consensus)

Module 2: **(10hrs.)**
Permissioned Blockchain(RAFT Consensus, Byzantine General Problem, Practical Byzantine Fault Tolerance), Blockchain for Enterprise - Overview, Blockchain Components and Concepts, Hyperledger Fabric – Transaction Flow, Hyperledger Fabric Details, Fabric – Membership and Identity Management, Hyperledger Fabric Network Setup, Fabric Demo on IBM Blockchain Cloud

Module 3: **(08hrs.)**
Hyperledger Composer – Application Development, Hyperledger Composer – Network Administration, Blockchain Use Cases, Blockchain in Financial Service(Payments and Secure Trading, Compliance and Mortgage, Financial Trade), Revolutionizing Global Trade, Blockchain in Supply Chain

Module 4: **(08hrs.)**
Blockchain in Other Industries, Blockchain in Government (Advantages, Use Cases, Digital Identity), Blockchain in Government(Hyperledger Indy, Tax Payments and Land Registry Records), Blockchain Security (Overview, Membership and Access control in Fabric, Privacy in Fabric)

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VIII Semester

Module 5: **(08hrs.)**

Blockchain Security(Fabric SideDB), Research Aspects(Consensus Scalability, Bitcoin-NG, Collective Signing, Byzcoin), Research Aspects (Algorand, Cross Fault Tolerance, Secured Multi-Party Computation), Blockchain for Science (Blockchain for Big Data, Blockchain and AI), Comparing Ecosystems – Ethereum

Course Outcome:

1. Explain the core concepts of blockchain technology, including its architecture, cryptographic foundations, and consensus mechanisms.
2. Implement and manage permissioned blockchain networks using Hyperledger Fabric, including transaction processing and identity management.
3. Evaluate real-world blockchain applications across multiple industries and assess their impact on financial services, trade, and governance.
4. Analyze and apply blockchain security principles, including privacy mechanisms, membership control, and threat mitigation strategies.
5. Investigate and compare emerging blockchain research topics, exploring innovations in consensus algorithms, scalability, and blockchain integration with AI and big data.

List of Text/ Reference Books:

1. Mastering Bitcoin: Unlocking Digital Cryptocurrencies, by Andreas Antonopoulos
2. Blockchain by Melanie Swa, O'Reilly
3. Hyperledger Fabric - https://www.hyperledger.org/projects/fabric
4. Zero to Blockchain - An IBM Redbooks course, by Bob Dill, David Smits
   https://www.redbooks.ibm.com/Redbooks.nsf/RedbookAbstracts/crse0401.html

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VIII Semester

PEC-CB04(C)	Natural Language Processing	3L:0T:0P (3hrs.)	3 Credits

Prerequisite: Engineering Mathematics, Theory of Computation

Course Objective: To gain the knowledge for developing advanced technology of computer systems like speech recognition and machine translation.

Course Contents: (40hrs)

Module 1: **(07 hrs.)**
Introduction to Natural Language Understanding- Levels of language analysis-Syntax, Semantics, Pragmatics, Applications, Ambiguity, Morphology, Parsing with Finite State Transducers, Regular Expressions, Stemmer, Spelling errors.

Module 2: **(10 hrs.)**
Computational Phonology: speech sound, phonetic transcription, text to speech, Pronunciation Variations, Bayesian Method to spelling and pronunciations, Minimum Edit Distance, Weighted Automata, N-grams.

Module 3: **(08 hrs.)**
HMM and speech recognition, Viterbi algorithm, Acoustic processing of speech, Feature Extraction, Speech Synthesis; Part-of-Speech Tagging: rule based, stochastic, transformation based.

Module 4: **(08 hrs.)**
Syntax Processing: Parsing with CFG, CKY parsing and the Earley parser, Probabilistic parsing; Semantic Processing: Meaning representation, First Order Predicate Calculus. Lexical Semantics: Internal structure of words, thematic roles, Primitive decomposition, WordNet.

Module 5: **(07 hrs.)**
Word sense disambiguation; Information Retrieval: Vector space model, Improving user queries; Pragmatic Processing: Discourse; Natural Language Generation, Machine Translation.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VIII Semester

Course Outcome:

1. To tag a given text with basic Language features
2. To design an innovative application using NLP components
3. To implement a rule based system to tackle morphology/syntax of a language
4 To design a tag set to be used for statistical processing for real-time applications
5. To compare and contrast the use of different statistical approaches for different types of NLP applications

List of Text Books / Reference Books:

1. D. Jurafsky and J.H. Martin, “Speech and Language Processing; Processing”, Prentice Hall, 2000.
2. C. Manning and H. Schutze, “Foundations of Statistical Natural Language Processing”, MIT Press
3. James Allen. “Natural Language Understanding”, Addison Wesley, 1994.
4. Richard M Reese, “Natural Language Processing with Javall”, OReilly Media, 2015.
5. Tanveer Siddiqui, U.S. Tiwary, “Natural Language Processing and Information Retrieval”, Oxford University Press, 2008

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VIII Semester

PEC-CB04(D)	Database Security	3L:0T:0P (3hrs.)	3 Credits

Prerequisite: Students should have an understanding of basic database concepts and mathematics

Course Contents: (40hrs)

Course Objective:
This course introduces the principles of database security, including database design, risk assessment, and architectural frameworks. It covers database vulnerabilities, security models, and mechanisms, along with strategies for managing threats, access control, and ensuring the integrity and confidentiality of information systems.

Course Content: (40 hrs.)

Module 1: (08Hrs)
Introduction:-Databases and Information Systems, An example usage context, Database system concepts and architecture, Overview of Information Security, Database design using the relational model Functional dependencies: Keys in a relational model, Concept of functional dependencies, Normal forms based on primary keys, BCNF Further Dependencies: Multi-values dependencies and fourth normal form, Join dependencies and fifth normal form, Inclusion dependencies, other dependencies and normal forms

Module 2: (08Hrs)
Database security lifecycle, data risk assessment, Analyze data threats, risks and vulnerabilities, Understand the need for a database security architecture, database security architecture, Implement a feedback mechanisms, Understand how to adjust policies and practices based on feedback mechanisms using different security models.

Module 3: (10Hrs)
Database Vulnerabilities, Threats and Physical Security: distinction between data and database security from network and perimeter security, external and internal database threats, flaws in perimeter security, risks of not securing an organization's data, typical database security hierarchy, analysis general security landscape, evaluation of security fundamentals, Understand the importance for staying current with database releases, fixes and security patches , Managing USB ports and USB enabled devices, Understand the implications of the physical placement of database files and their copies.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VIII Semester

Module 4: **(08Hrs)**

Security Models - Bell and LaPadula's Model Biba's Model Dion's Model Sea View Model Jajodia and Sandhu's Model The Lattice Model for the Flow Control conclusion Security Mechanisms Introduction User Identification/Authentication Memory Protection Resource Protection Control Flow Mechanisms Isolation Security Functionalities in Some Operating Systems Trusted Computer System Evaluation

Module 5: **(06Hrs)**

Security Management, Data/ information, protecting Password file, Access Control Structure, Software Security, Element of Information Security, Steps for Better Security, Malicious Software, System Security Assurance Concepts, Importance of Information System.

Course outcomes:

1. Understand database design principles and normalization techniques to model secure and efficient relational databases.
2. Analyze database security architecture and lifecycle, including threat and risk assessment, and implement security policies using established models.
3. Identify and address database vulnerabilities and physical security risks through evaluation of threats, patches, and best practices in securing data assets.
4. Apply formal security models and mechanisms such as Bell-LaPadula, Biba, and Lattice models for controlling access and ensuring data confidentiality and integrity.
5. Implement effective security management practices, including access control, password protection, malware defense, and system security assurance.

Text Books:

1. Handbook of Database Security: Applications and Trends by Michael Gertz and SushilJajodia
2. Database Security and Auditing, Hassan A. Afyouni, India Edition, CENGAGE Learning, 2009.
3. Database Security, Castano, Second edition, Pearson Education
4. Database security by alfred basta, melissazgola, CENGAGE learning
5. H. F. Korthand A.Silberschatz .Database Concept, TMH.
6. Godbole, “Information system security”, Wiley.
7. Cole. Krutz&Conley “Network security”Wiley

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VIII Semester

PEC-CB05(A)	Mobile & Wireless Security	3L:0T:0P (3hrs.)	3 Credits

Prerequisite: NA.

Course Objectives: This course aims to provide students with foundational and advanced knowledge of wireless and mobile networking technologies, covering evolving wireless standards, mobile IP, 3G/4G systems, and security models. It also explores secure wireless communication and electronic transactions in e-commerce and m-commerce environments.

Course Contents: (40 hrs.)

Module 1: **(08 hrs.)**
Wireless Networking Trends, Key Wireless Physical Layer Concepts, Wireless Local Area Networks, Wireless Personal Area Networks, WiMAX (Physical layer, Media access control, Mobility and Networking)

Module 2: **(08 hrs.)**
Mobile IPv4, Mobile IPv6, TCP over Wireless Networks, Ad Hoc Networks - Issues and Routing, Wireless Sensor Networks, Wireless Mesh and Multi-Hop Relay Networks.

Module 3: **(08 hrs.)**
3G and 4G Network, General Packet Radio Services (GPRS), Universal Mobile Telecommunication System (UMTS).Radio Frequency Identification (RFID).

Module 4: **(08 hrs.)**
Introduction to LTE, Security Issues in Wireless Networks, Security Models: Military and civil security, vulnerability and threat models, End-end Security, link encryption, compartments Privacy. Authentication. Denial of service. Nonrepudiation. Issues in multi-level secure systems. Internet security models: IPv4/IPv6 encapsulation header.

Module 5: **(08 hrs.)**
E-Commerce, M-Commerce, Electronic payment systems, electronic cards, Secure Electronic Transactions: Trust, Encryption, Authentication, confidentiality, integrity and nonrepudiation.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VIII Semester

Course Outcome:

1. Understand the architecture, trends, and physical layer concepts of various wireless communication technologies including WLAN, WPAN, and WiMAX.
2. Analyze mobility protocols such as Mobile IPv4/IPv6 and evaluate routing challenges in Ad Hoc, Sensor, and Mesh networks.
3. Explain the structure and functioning of mobile communication systems including GPRS, UMTS, 3G, 4G, and RFID technologies.
4. Evaluate security models and mechanisms used in wireless networks to ensure privacy, authentication, and integrity across different layers.
5. Apply secure transaction principles in e-commerce and m-commerce platforms using encryption, digital signatures, and electronic payment systems.

List of Text / Reference Books:

1. Stalling W. " Network Security Essentials", Pearson
2. Practical Packet Analysis: Using Wireshark to Solve Real-Word Network problems by Chris Sanders
3. Jochen Schiller, "Mobile Communications", PHI.
4. Uwe Hansmann, LotharMerk, Martin S. Nicklons and Thomas Stober, Principles of Mobile Computing, Springer, New York, 2003
5. Frank Adelstein, Sandeep KS Gupta, Golden Richard, Fundamentals of Mobile and Pervasive Computing, McGraw-Hill

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VIII Semester

PEC-CB05(B)	Knowledge Management	3L:0T:0P (3hrs.)	3 Credits

Prerequisite: NA

Course Objective: Learn the Evolution of Knowledge management, familiar with tools, exposed to Applications, familiar with some case studies.

Course Contents: (40 hrs.)

Module 1: **(10 hrs.)**
Introduction: An Introduction to Knowledge Management–The foundations of knowledge management- including cultural issues-technology applications organizational concepts and processes-management aspects-and decision support systems. The Evolution of Knowledge management: From Information Management to Knowledge Management–Key Challenges Facing the Evolution of Knowledge Management–Ethics for Knowledge Management.

Module 2: **(06 hrs.)**
Organization and Knowledge Management –Building the Learning Organization. Knowledge Markets: Cooperation among Distributed Technical Specialists–Tacit Knowledge and Quality Assurance.

Module 3: **(08 hrs.)**
Telecommunications and Networks in Knowledge Management–Internet Search Engines and Knowledge Management–Information Technology in Support of Knowledge Management–Knowledge Management and Vocabulary Control–Information Mapping in Information Retrieval– InformationCodingintheInternetEnvironment–RepackagingInformation.

Module 4: **(08 hrs.)**
Components of a Knowledge Strategy–Case Studies (From Library to Knowledge Center, Knowledge Management in the Health Sciences, Knowledge Management in Developing Countries).

Module 5: **(08 hrs.)**
Advanced topics and case studies in knowledge management–Development of acknowledge management map/plan that is integrated with an organization's strategic and business plan–A case study on Corporate Memories for supporting various aspects in the process life-cycles of an organization.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)

Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VIII Semester

Course Outcome:

1. Describe how valuable individual, group and organizational knowledge is managed throughout the knowledge management cycle.
2. Define the different knowledge types and explain how they are addressed by knowledge management.
3. Describe them a major roles and responsibilities in knowledge management implementations.
4. Identify some of the key tools and technique used in knowledge management applications.
5. Identify and evaluate major KM issues such as ethics, knowledge owner ship vs. authorship, copyright, intellectual property and knowledge sharing incentives.

List of Text / Reference Books:

1. Srikantaiah,T.K., Koenig,M., "Knowledge Management for the Information Professional "Information Today,Inc.,2000.
2. Nonaka,I., Takeuchi,H.,"TheKnowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation",OxfordUniversityPress,1995.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VIII Semester

PEC-CB05(C)	Data Visualization	3L:0T:0P (3hrs.)	3 Credits

Prerequisite: Computer Graphics and Multimedia

Course Objective: To understand the various types of data, apply and evaluate the principles of data visualization. Acquire skills to apply visualization techniques to a problem and its associated dataset.

Course Contents: (40 hrs.)

Module 1: **(06 hrs.)**
Introduction to Data Visualization: Overview of data Visualization-Data Abstraction -Analysis: Four Levels for Validation-Task Abstraction-Analysis: Four Levels for Validation.

Module 2: **(10 hrs.)**
Visualization Techniques Scalar and point techniques Color Maps Contouring Height Plots-Vector visualization techniques Vector Properties Vector Glyphs Vector Color Coding Stream Objects.

Module 3: **(10 hrs.)**
Visual Analytics: Visual Variables-Networks and Trees-Map Color and Other Channels-Manipulate View, Arrange Tables Geo Spatial Data Reduce Items and Attributes.

Module 4: **(08 hrs.)**
Visualization Tools and Techniques: Introduction to data visualization Tools-Tableau-Visualization using R.

Module 5: **(06 hrs.)**
Diverse Types of Visual Analysis Time-Series data visualization Text data visualization Multi variate data visualization and case studies. Dash board create

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VIII Semester

Course Outcome:

1. Identify the different data types, visualization types to bring out the insight. Relate the visualization towards the problem based on the dataset.
2. Identify the different attributes and show casing the min plots.
3. Identify and create various visualizations for geospatial and table data.
4. Ability to visualize categorical, quantitative and text data.
5. Illustrate the integration of visualization tools with Hadoop. Ability to visualize categorical, quantitative and text data.

List of Text / Reference Books:

1. Tamara Munzer, Visualization Analysis and Design-, CRC Press 2014
2. Alexandru Telea, Data Visualization Principles and Practice CRC Press 2014.
3. Paul J. Deitel, Harvey Deitel, Java SE8 for Programmers (Deitel Developer Series) 3rd Edition, 2014.
4. Y.Daniel Liang, Introduction to Java programming-comprehensive version Tenth Edition, Pearson ltd 2015.
5. Paul Deitel Harvey Deitel, Java, How to Program, PrenticeHall;9thedition,2011.
6. Cay Horstmann BIG JAVA,4thedition, John WileySons,2009
7. Nicholas S. Williams, Professional Java for Web Applications, WroxPress,2014.

List of Experiments:

1. Acquiring and plotting data.
2. Statistical Analysis such as Multivariate Analysis, PCA, LDA, Correlation, regression and analysis of variance.
3. Time-series analysis stock market. Visualization on Streaming dataset.
4. Dashboard Creation. Text visualization

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VIII Semester

PEC-CB05(D)	**Data Mining and Warehousing**	**3L:0T:0P (3hrs.)**	**3 Credits**

Prerequisite: Computer Organization & Architecture

Course Objective: Student should understand the value of Historical data and data mining in solving real- world problems.

Course Contents: (40 hrs.)

Module 1: **(10 hrs.)**
Data Warehousing: Introduction, Delivery Process, Data warehouse Architecture, Data Preprocessing: Data cleaning, Data Integration and transformation, Data reduction. Data warehouse Design: Data warehouse schema, Partitioning strategy Data Warehouse Implementation, Data Marts, Meta Data, Example of a Multidimensional Data model. Introduction to Pattern Warehousing.

Module 2: **(08 hrs.)**
OLAP Systems: Basic concepts, OLAP queries, Types of OLAP servers, OLAP operations etc. Data Warehouse Hardware and Operational Design: Security, Backup and Recovery

Module 3: **(08 hrs.)**
Introduction to Data & Data Mining: Data Types, Quality of data, Data Preprocessing, Similarity measures, Summary statistics, Data distributions, Basic data mining tasks, Data Mining V/s knowledge discovery in databases. Issues in Data mining. Introduction to Fuzzy set sand fuzzy logic.

Module 4: **(08 hrs.)**
Supervised Learning: Classification: Statistical-based algorithms, Distance-based algorithms, Decision tree-based algorithms, neural network-based algorithms, Rule-based algorithms, and Probabilistic Classifiers.

Module 5: **(06 hrs.)**
Clustering & Association Rule mining: Hierarchical algorithms, Partitioned algorithms, Clustering large databases–BIRCH, DBSCAN, CURE algorithms. Association rules: Parallel and distributed algorithms such as A priori and FP growth algorithms.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VIII Semester

Course Outcome:

1. Understand the need of designing Enterprise data warehouses and will be enabled to approach business problems analytically by identifying opportunities to derive business.
2. Compare and contrast various methods for storing & retrieving data from different data sources/repository.
3. As certain the application of data mining in various areas and preprocess the given data and visualize it for a given application or data exploration/mining task.
4. Apply supervised learning methods to given data sets such as classification and its various types.
5. Apply Unsupervised learning methods to given data sets such as clustering and its various types. Also apply Association rule mining to various domains.

List of Text / Reference Books:

1. Pennington, Steinbach & Kumar, “Introduction to Data mining”, Pearson Edu, 2019.
2. Jaiwei Han, Micheline Kamber, “Datamining: Concepts and Techniques”, Morgan Kaufmann Publishers.
3. Margaret H. Dunham, “Datamining: Introductory and Advanced topics”, PearsonEdu.2009.
4. Anahory & Murray, “Data Warehousing i n t h e Real-world”, Pearson Edu. 2009

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VIII Semester

PEC-CB05(E)	**Information Systems & Infrastructure Security Management**	**3L:0T:0P (3hrs.)**	**3 Credits**

Pre-requisite: Computer Network, Network Security essentials, Knowledge of Network Operating System.

Course Objective: This course covers physical and logical cybersecurity for data centers and IT infrastructures. It defines a management program to protect assets across all levels of technology and the core components that support that information technology.

Course Contents: (40 hrs.)

Module 1: **(08hrs.)**
IT infrastructure Introduction, challenges, design issues in IT organization and IT infrastructure, Determining customer's requirements, IT systems, management process, IT service management process, Information system design process, patterns for IT systems management, IT infrastructure library.

Module 2: **(10hrs.)**
Security Management: Computer and Internet Security, Physical Security, Identity Management, Access Management, Intrusion Detection, Security Information Management. IT Ethics: Cyber Ethics, Intellectual Property, Privacy and Law, Computer Forensics, Ethics and Internet, Cyber Crimes

Module 3: **(10hrs.)**
Data Center Infrastructure: Data Center Infrastructure Architecture Overview - Data Center –site location and site configuration, Various Elements in a Data centre-their functions, Hardware and Software Recommendations, Software Recommendations, Data Center Multi-Layer Design, Network Management.

Module 4: **(06hrs.)**
Data Center Security: Security aspects in a Data Centre, Packet Filtering: Aggregation Layer, Packet Filtering: Access Layer, Security for Multi-Tier Server Farms, Intrusion Detection Sensors

Module 5: **(06hrs.)**
Virtual Data Centre: What is a Virtual data Centre, Virtual Data Centre management, Remote management.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)

Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VIII Semester

Course Outcome:

1. Understand data security to application level security.
2. Define Security Management like: Internet, physical and IT Ethics.
3. Understand basic aspects of architecture, design of Data Center.
4. Understand basic aspects of security of Data Center.
5. Understanding Virtual Data Centre.

List of Text/ Reference Books:

1. CCNA Cisco Certified Network Associate Study Guide - Richard Deal.
2. Data Center Fundamentals" by Mauricio Arregoces, Maurizio Portolani, Cisco Press 2003. ISBN 1587050234.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VIII Semester

SBC-CB03(P)	**Penetration Testing and Vulnerability Analysis Lab**	**0L:0T:4P (4hrs.)**	**2 Credits**

Pre-requisite: Computer networks and operating systems (Windows/Linux), Fundamental cyber security concepts (CIA triad, threat types, etc.)

Course Objective: 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.

Course Contents: (40 hrs.)

Module 1: **(08hrs.)**
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.

Module 2: **(08hrs.)**
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.

Module 3: **(08hrs.)**
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.

Module 4: **(08hrs.)**
Cryptography and Secure Communications: Basics of cryptography, Cryptographic algorithms and protocols, Encryption, decryption, and key management, secure communication channels Reporting and Remediation: Documentation and reporting of findings, Prioritizing and mitigating

vulnerabilities, engaging stakeholders and communicating recommendations, post-testing activities and continuous improvement.

Module 5: **(08hrs.)**

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.

Course Outcome:

1. Demonstrate the ability to gather intelligence and scan networks using ethical penetration testing methodologies.
2. Identify and exploit vulnerabilities in systems and web applications, and perform post-exploitation activities effectively.
3. Assess and test wireless networks and social engineering vulnerabilities to enhance organizational security posture.
4. Apply cryptographic techniques and document penetration testing findings with appropriate remediation strategies.
5. Perform comprehensive penetration tests across mobile, cloud, and IoT environments, and showcase skills through practical simulations and projects.

Text/Reference 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"

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VIII Semester

PROJ-CB06(A)	Project-III	0L:0T:16P (16hrs.)	8 Credits

Prerequisite: Fundamentals of Cybersecurity, Internet of Things, Blockchain Technology (e.g., consensus mechanisms, smart contracts, distributed ledger systems), Basic Programming & Networking Concepts, equivalent mini-project experience.

Course Objective:

This course aims to enable students to apply their knowledge of Cybersecurity, IoT, and Blockchain by working on a comprehensive project, enhancing problem-solving skills, fostering teamwork, and preparing them for careers in industry and research with hands-on experience in project management and innovation. Students will also develop research, design, and implementation capabilities in secure computing, smart technologies, and decentralized systems.

Course Outcome:

1. Design and develop an industry-relevant project using Cybersecurity, IoT, or Blockchain technologies.
2. Apply advanced engineering concepts to build secure, scalable, and efficient systems in emerging technology domains.
3. Analyze complex problems and implement innovative solutions with a structured approach in project development.
4. Demonstrate teamwork, leadership, and professional ethics while working collaboratively on a project.
5. Effectively document and present project findings through technical reports, research papers, and oral presentations.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VIII Semester

PROJ-CB06(A)	**Internship and Project (Industry/Corporate/Academia)**	**0L:0T:16P (16hrs.)**	**8 Credits**

Prerequisite:

Course Objective:
This course aims to provide hands-on industry exposure in cybersecurity, IoT, and blockchain, while developing problem-solving and technical skills through real-world projects. It fosters teamwork, communication, and professional ethics, preparing students for industry readiness by strengthening their ability to design and evaluate solutions in emerging technology domains.

Course Outcomes:

1. Demonstrate industry-relevant skills by successfully completing an internship/project in cybersecurity, IoT, or blockchain technology.
2. Apply advanced concepts of cybersecurity, IoT, and blockchain in designing, developing, and optimizing innovative solutions.
3. Analyze real-world problems and propose effective technological solutions using a structured approach in an industry or academic setting.
4. Work effectively in a team environment and exhibit professional ethics, project management skills, and effective communication.
5. Present and document project findings in a structured format, showcasing their ability to contribute to research and development in their chosen domain.