JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B.Tech. in CSE (CYBER SECURITY)
III & IV YEAR COURSE STRUCTURE & TENTATIVE SYLLABUS (R18)

Applicable From 2020-21 Admitted Batch

III YEAR I SEMESTER

S. No.	Course Code	Course Title	L	T	P	Credits
1		Design and Analysis of Algorithms	3	0	0	3
2		Cryptography and Network Security	3	0	0	3
3		Database Management Systems	3	0	0	3
4		Formal Languages and Automata Theory	3	0	0	3
5		Professional Elective - I	3	0	0	3
6		Professional Elective - II	3	0	0	3
7		Cryptography and Network Security Lab	0	0	3	1.5
8		Database Management Systems Lab	0	0	3	1.5
9		Advanced Communication Skills Lab	0	0	2	1
10		Intellectual Property Rights	3	0	0	0
		Total Credits	**21**	**0**	**8**	**22**

III YEAR II SEMESTER

S. No.	Course Code	Course Title	L	T	P	Credits
1		Cyber Security	3	1	0	4
2		Cyber Crime Investigation & Digital Forensics	3	1	0	4
3		Software Engineering	3	1	0	4
4		Professional Elective – III	3	0	0	3
5		Open Elective - I	3	0	0	3
6		Cyber Security Lab	0	0	3	1.5
7		Cyber Crime Investigation & Digital Forensics Lab	0	0	3	1.5
8		Professional Elective – III Lab	0	0	2	1
9		Environmental Science	3	0	0	0
		Total Credits	**18**	**3**	**8**	**22**

IV YEAR I SEMESTER

S. No.	Course Code	Course Title	L	T	P	Credits
1		Vulnerability Assessment & Penetration Testing	3	0	0	3
2		Network Management Systems and Operations	2	0	0	2
3		Professional Elective - IV	3	0	0	3
4		Professional Elective - V	3	0	0	3
5		Open Elective - II	3	0	0	3
6		Vulnerability Assessment & Penetration Testing lab	0	0	2	1
7		Industrial Oriented Mini Project / Summer Internship	0	0	0	2*
8		Seminar	0	0	2	1
9		Project Stage - I	0	0	6	3
		Total Credits	**14**	**0**	**10**	**21**

IV YEAR II SEMESTER

S. No.	Course Code	Course Title	L	T	P	Credits
1		Organizational Behaviour	3	0	0	3
2		Professional Elective - VI	3	0	0	3
3		Open Elective - III	3	0	0	3
4		Project Stage - II	0	0	14	7
		Total Credits	**9**	**0**	**14**	**16**

*Note: Industrial Oriented Mini Project/ Summer Internship is to be carried out during the summer vacation between 6th and 7th semesters. Students should submit report of Industrial Oriented Mini Project/ Summer Internship for evaluation.

MC - Environmental Science – Should be Registered by Lateral Entry Students Only.
MC – Satisfactory/Unsatisfactory.

Professional Elective - I

	Compiler Design
	Artificial Intelligence
	Data warehousing and Data Mining
	Ad-hoc & Sensor Networks
	Cloud Computing

Professional Elective - II

	Ethical Hacking
	Data Science
	Distributed Systems
	Cyber Laws
	IoT Security

Professional Elective - III

	Mobile Application Security
	Machine Learning
	DevOps
	Mobile Application Development
	Blockchain Technology

 # Courses in PE - III and PE - III Lab must be in 1-1 correspondence.

Professional Elective - IV

	Edge Analytics
	Web & Database Security
	Computer Security & Audit Assurance
	Social Media Security
	Deep Learning

Professional Elective - V

	Quantum Computing
	Data Analytics for Fraud Detection
	5G Technologies
	Security Incident & Response Management (SOC)
	Authentication Techniques

Professional Elective – VI

	Quantum Cryptography
	IoT Cloud Processing and Analytics
	Cloud Security
	Digital Watermarking and Steganography
	Data Privacy

ORGANIZATIONAL BEHAVIOUR

B.Tech. IV Year II Sem.   L T P C
                                                              3 0 0 3

Course Objectives: The objective of the course is to provide the students with the conceptual framework and the theories underlying Organizational Behavior.

Course Outcomes:
1. Demonstrate the applicability of analyzing the complexities associated with management of individual behavior in the organization.
2. Analyze the complexities associated with management of the group behavior in the organization.
3. Demonstrate how the organizational behavior can integrate in understanding the motivation (why) behind behavior of people in the organization.

UNIT - I:
Introduction to OB - Definition, Nature and Scope – Environmental and organizational context – Impact of IT, globalization, Diversity, Ethics, culture, reward systems and organizational design on Organizational Behaviour. Cognitive Processes-I: Perception and Attribution: Nature and importance of Perception – Perceptual selectivity and organization – Social perception – Attribution Theories – Locus of control –Attribution Errors –Impression Management.

UNIT- II:
Cognitive Processes-II: Personality and Attitudes – Personality as a continuum – Meaning of personality - Johari Window and Transactional Analysis - Nature and Dimension of Attitudes – Job satisfaction and organizational commitment-Motivational needs and processes- Work-Motivation Approaches Theories of Motivation- Motivation across cultures - Positive organizational behaviour: Optimism – Emotional intelligence – Self-Efficacy.

UNIT - III:
Dynamics of OB-I: Communication – types – interactive communication in organizations – barriers to communication and strategies to improve the follow of communication - Decision Making: Participative decision-making techniques – creativity and group decision making. Dynamics of OB –II Stress and Conflict: Meaning and types of stress –Meaning and types of conflict - Effect of stress and intra-individual conflict - strategies to cope with stress and conflict.

UNIT - IV:
Dynamics of OB –III Power and Politics: Meaning and types of power – empowerment - Groups Vs. Teams – Nature of groups – dynamics of informal groups – dysfunctions of groups and teams – teams in modern work place.

UNIT - V:
Leading High performance: Job design and Goal setting for High performance- Quality of Work Life-Socio technical Design and High-performance work practices - Behavioural performance management: reinforcement and punishment as principles of Learning –Process of Behavioural modification - Leadership theories - Styles, Activities and skills of Great leaders.

REFERENCE BOOKS:
1. Luthans, Fred: Organizational Behaviour 10/e, McGraw-Hill, 2009
2. McShane: Organizational Behaviour, 3e, TMH, 2008
3. Nelson: Organizational Behaviour, 3/e, Thomson, 2008.

4. Newstrom W. John & Davis Keith, Organisational Behaviour-- Human Behaviour at Work, 12/e, TMH, New Delhi, 2009.
5. Pierce and Gardner: Management and Organisational Behaviour: An Integrated perspective, Thomson, 2009.
6. Robbins, P. Stephen, Timothy A. Judge: Organisational Behaviour, 12/e, PHI/Pearson, New Delhi, 2009.
7. Pareek Udai: Behavioural Process at Work: Oxford & IBH, New Delhi, 2009.
8. Schermerhorn: Organizational Behaviour 9/e, Wiley, 2008.
9. Hitt: Organizational Behaviour, Wiley, 2008
10. Aswathappa: Organisational Behaviour, 7/e, Himalaya, 2009
11. Mullins: Management and Organisational Behaviour, Pearson, 2008.
12. McShane, Glinow: Organisational Behaviour--Essentials, TMH, 2009.
13. Ivancevich: Organisational Behaviour and Management, 7/e, TMH, 2008.

QUANTUM CRYPTOGRAPHY (Professional Elective – VI)

B.Tech. IV Year II Sem.

	L	T	P	C
	3	0	0	3

Course Objectives: Objective of the course is to build quantum-preparedness for the post quantum era.

Course Outcomes:
1. Basic understanding about Quantum Information and Computation.
2. Understand attack Strategies on QKD Protocols.
3. Analyze and understand statistical analysis of QKD Networks in Real-Life Environment.
4. Apply Quantum-cryptographic networks.

UNIT - I
Quantum Information Theory, Unconditional Secure Authentication, Entropy, Quantum Key Distribution, Quantum Channel, Public Channel, QKD Gain, Finite Resources

UNIT - II
Adaptive Cascade Introduction, Error Correction and the Cascade Protocol, Adaptive Initial Block-Size Selection, Fixed Initial Block-Size, Dynamic Initial Block-Size, Examples

UNIT - III
Attack Strategies on QKD Protocols: Introduction, Attack Strategies in an Ideal Environment, Individual Attacks in an Realistic Environment QKD Systems: Introduction, QKD Systems

UNIT - IV
Statistical Analysis of QKD Networks in Real-Life Environment: Statistical Methods, Statistical Analysis QKD Networks Based on Q3P: QKD Networks, PPP, Q3P, Routing, Transport

UNIT - V
Quantum-Cryptographic Networks from a Prototype to the Citizen: The SECOQC Project, How to Bring QKD into the "Real" Life The Ring of Trust Model: Introduction, Model of the Point of Trust, Communication in the Point of Trust Model, Exemplified Communications, A Medical Information System Based on the Ring of Trust

TEXT BOOK:
1. Kollmitzer C., Pivk M. (Eds.), Applied Quantum Cryptography, Lect. Notes Phys. 797 (Springer, Berlin Heidelberg 2010).

REFERENCE BOOKS:
1. Gerald B. Gilbert, Michael Hamrick, and Yaakov S. Weinstein, Quantum Cryptography, World Scientific Publishing.
2. Gilles Van Assche, Quantum Cryptography and Secret-Key Distillation, Cambridge University Press.

IOT CLOUD PROCESSING AND ANALYTICS (Professional Elective – VI)

B.Tech. IV Year II Sem.	**L**	**T**	**P**	**C**
	3	**0**	**0**	**3**

Course Objectives: Knowledge on IoT networking connectivity protocols and IoT Analytics for the cloud processing.

Course Outcomes: At the end of the course, students will be able to:
1. Implement the architectural components and protocols for application development.
2. Identify data analytics and data visualization tools as per the problem characteristics.
3. Collect, store and analyze IoT data.

UNIT - I
IoT devices, Networking basics, IoT networking connectivity protocols, IoT networking data messaging protocols, Analyzing data to infer protocol and device characteristics.

UNIT - II
IoT Analytics for the Cloud: Introduction to elastic analytics, Decouple key components, Cloud security and analytics, Designing data processing for analytics, Applying big data technology to storage.

UNIT - III
Exploring IoT Data: Exploring and visualizing data, Techniques to understand data quality, Basic time series analysis, Statistical analysis.

UNIT - IV
Data Science for IoT Analytics: Introduction to Machine Learning, Feature engineering with IoT data, Validation methods, Understanding the bias–variance tradeoff, Use cases for deep learning with IoT data.

UNIT - V
Strategies to Organize Data for Analytics: Linked Analytical Datasets, Managing data lakes, data retention strategy.

TEXT BOOKS:
1. Arshdeep Bahga and Vijay Madisetti, "Internet of Things – A Hands on Approach", Universities Press, 2015.
2. Kevin, Townsend, Carles, Cufí, Akiba and Robert Davidson, "Getting Started with Bluetooth Low Energy" O'Reilly.

REFERENCE BOOKS:
1. Madhur Bhargava "IoT Projects with Bluetooth Low Energy, Packt Publishing, August 2017.
2. Robin Heydon," Bluetooth Low Energy: The Developer's Handbook", Pearson, October 2012.
3. Kumar Saurabh," Cloud Computing", Wiley India, 1st Edition, 2016.

CLOUD SECURITY (Professional Elective – VI)

B.Tech. IV Year II Sem.　　　　　　　　　　　　　　　　　　　　　　**L　T　P　C**
　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　3　0　0　3

Pre-requisites: Computer Networks, Cryptography and Network Security, Cloud Computing.

Course Objectives:
1. To understand the fundamentals concepts of cloud computing.
2. To understand the cloud security and privacy issues.
3. To understand the Threat Model and Cloud Attacks.
4. To understand the Data Security and Storage.
5. To analyze Security Management in the Cloud.

Course Outcome
1. Ability to acquire the knowledge on fundamentals concepts of cloud computing.
2. Able to distinguish the various cloud security and privacy issues.
3. Able to analyze the various threats and Attack tools.
4. Able to understand the Data Security and Storage.
5. Able to analyze the Security Management in the Cloud.

UNIT - I
Overview of Cloud Computing: Introduction, Definitions and Characteristics, Cloud Service Models, Cloud Deployment Models, Cloud Service Platforms, Challenges Ahead.
Introduction to Cloud Security: Introduction, Cloud Security Concepts, CSA Cloud Reference Model, NIST Cloud Reference Model, NIST Cloud Reference Model.
Note: Laboratory practice will be imparted with the help of relevant case studies as and when required.

UNIT - II
Cloud Security and Privacy Issues: Introduction, Cloud Security Goals/Concepts, Cloud Security Issues, Security Requirements for Privacy, Privacy Issues in Cloud.
Infrastructure Security: The Network Level, the Host Level, the Application Level, SaaS Application Security, PaaS Application Security, IaaS Application Security.
Note: Laboratory practice will be imparted with the help of relevant case studies as and when required.

UNIT - III
Threat Model and Cloud Attacks: Introduction, Threat Model- Type of attack entities, Attack surfaces with attack scenarios, A Taxonomy of Attacks, Attack Tools-Network-level attack tools, VM-level attack tools, VMM attack tools, Security Tools, VMM security tools.
Note: Laboratory practice will be imparted with the help of relevant case studies as and when required.

UNIT - IV
Information Security Basic Concepts, an Example of a Security Attack, Cloud Software Security Requirements, Rising Security Threats. **Data Security and Storage:** Aspects of Data Security, Data Security Mitigation, Provider Data and Its Security.
Note: Laboratory practice will be imparted with the help of relevant case studies as and when required.

UNIT - V
Evolution of Security Considerations, Security Concerns of Cloud Operating Models, Identity Authentication, Secure Transmissions, Secure Storage and Computation, Security Using Encryption Keys, Challenges of Using Standard Security Algorithms, Variations and Special Cases for Security Issues with Cloud Computing, Side Channel Security Attacks in the Cloud

Security Management in the Cloud- Security Management Standards, Availability Management, Access Control, Security Vulnerability, Patch, and Configuration Management.

Note: Laboratory practice will be imparted with the help of relevant case studies as and when required.

TEXT BOOKS:
1. Cloud Security Attacks, Techniques, Tools, and Challenges by Preeti Mishra, Emmanuel S Pilli, Jaipur R C Joshi Graphic Era, 1st Edition published 2022 by CRC press.
2. Cloud Computing with Security Concepts and Practices Second Edition by Naresh Kumar Sehgal Pramod Chandra, P. Bhatt John M. Acken,2nd Edition Springer nature Switzerland AG 2020.
3. Cloud Security and Privacy by Tim Mather, Subra Kumaraswamy, and Shahed Lati First Edition, September 2019.

REFERENCE BOOKS:
1. Essentials of Cloud Computing by K. Chandrasekaran Special Indian Edition CRC press.
2. Cloud Computing Principles and Paradigms by Rajkumar Buyya, John Wiley.

DIGITAL WATERMARKING AND STEGANOGRAPHY (Professional Elective – VI)

B.Tech. IV Year II Sem.

L	T	P	C
3	0	0	3

Course Objectives:
1. To learn about the watermarking models and message coding.
2. To learn about watermark security and authentication.
3. To learn about steganography. Perceptual models.

Course Outcomes:
1. Know the History and importance of watermarking and steganography.
2. Analyze Applications and properties of watermarking and steganography.
3. Demonstrate Models and algorithms of watermarking.
4. Possess the passion for acquiring knowledge and skill in preserving authentication of Information.
5. Identify theoretic foundations of steganography and steganalysis.

UNIT - I
Introduction: Information Hiding, Steganography and Watermarking – History of watermarking – Importance of digital watermarking – Applications – Properties – Evaluating watermarking systems.
Watermarking models & message coding: Notation – Communications – Communication based models – Geometric models – Mapping messages into message vectors – Error correction coding – Detecting multi-symbol watermarks.

UNIT - II
Watermarking with side information & analyzing errors: Informed Embedding – Informed Coding – Structured dirty-paper codes - Message errors – False positive errors – False negative errors – ROC curves – Effect of whitening on error rates.

UNIT - III
Perceptual models: Evaluating perceptual impact – General form of a perceptual model – Examples of perceptual models – Robust watermarking approaches - Redundant Embedding, Spread Spectrum Coding, Embedding in Perceptually significant coefficients.

UNIT - IV
Watermark security & authentication: Security requirements – Watermark security and cryptography – Attacks – Exact authentication – Selective authentication – Localization –Restoration.

UNIT - V
Steganography: Steganography communication – Notation and terminology – Information Theoretic Foundations of steganography – Practical steganographic methods – Minimizing the embedding impact – Steganalysis

TEXT BOOK:
1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, "Digital Watermarking and Steganography", Margan Kaufmann Publishers, New York, 2008.

REFERENCE BOOK:
1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, "Digital Watermarking", Margan Kaufmann Publishers, New York, 2003.

DATA PRIVACY (Professional Elective – VI)

B.Tech. IV Year II Sem.   L T P C
                                                                                               3 0 0 3

Course Objectives:
1. The objective of this course is to create architectural, algorithmic and technological foundations for the maintenance of the privacy of individuals.
2. Students are able to learn the concepts of confidentiality of organizations, and the protection of sensitive information, despite the requirement that information be released publicly or semi-publicly.

Course Outcomes:
1. Discuss the concepts of privacy in today's environment.
2. How automation is changing the concepts and expectations concerning privacy and the increasingly interconnected issue of security.
3. Explain the knowledge of the role of private regulatory and self-help efforts.
4. How emerging issues are affecting society and business, with a concentration on how information security must shape corporate practices.

UNIT - I:
Introduction- Fundamental Concepts, Definitions, Statistics, Data Privacy Attacks, Data linking and profiling, access control models, role-based access control, privacy policies, their specifications, languages and implementation, privacy policy languages, privacy in different domains- medical, financial, etc.

UNIT - II:
Data explosion- Statistics and Lack of barriers in Collection and Distribution of Person- specific information, Mathematical model for characterizing and comparing real-world data sharing practices and policies and for computing privacy and risk measurements, Demographics and Uniqueness, **Protection Models**- Null-map, k-map, Wrong map

UNIT - III:
Survey of techniques- Protection models (null-map, k-map, wrong map), Disclosure control, Inferring entity identities, Strength and weaknesses of techniques, entry specific databases.

UNIT - IV:
Computation systems for protecting delimited data- MinGen, Datafly, Mu-Argus, k- Similar, Protecting textual documents: Scrub.

UNIT - V:
Technology, Policy, Privacy and Freedom- Medical privacy legislation, policies and best practices, Examination of privacy matters specific to the World Wide Web, Protections provided by the Freedom of Information Act or the requirement for search warrants.

TEXT BOOKS:
1. B. Raghunathan, The Complete Book of Data Anonymization: From Planning to Implementation, 1st Edition, Auerbach Pub, 2013.
2. L. Sweeney, Computational Disclosure Control: A Primer on Data Privacy Protection, MIT Computer Science, 2002.

REFERENCE BOOKS:
1. Nishant Bhajaria Data Privacy: A runbook for engineers, Manning Publications.
2. Gwen Kennedy, Data Privacy Law: A Practical Guide to the GDPR, ISBN-13: 978-0999512722, ISBN-10: 0999512722.