Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

ACADEMIC REGULATIONS

CURRICULUM STRUCTURE

and

DETAILED SYLLABUS

for

Two Year PG Programme

in

M. Tech. (Cyber Security)

(Applicable for batches admitted from 2019)

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

VISION OF THE INSTITUTE

To be a premier institute of excellence developing highly talented holistic human capital that contributes to the nation through leadership in technology and innovation through engineering education.

MISSION OF THE INSTITUTE

1. To impart Personnel Skills and Ethical Values for Sustainable Development of the Nation.
2. To create Research & Industry oriented centers of excellence in all engineering disciplines.
3. To be a renowned IPR generator and repository for innovative technologies.
4. To develop Research and Industry oriented technical talent.
5. To benchmark globally the academic & research output.

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

VISION OF THE DEPARTMENT

Department of Computer Science and Engineering strives rigorously to impart intellectual environment with global standards that fosters the search for new knowledge in a highly dynamic computing-centric society through research & applied efforts.

MISSION OF THE DEPARTMENT

- To provide quality education in both theoretical and applied foundations of computer science and train the students to solve the real world problems effectively thus enhancing their potential for high quality careers.
- To facilitate the students and faculty to inculcate the research culture to advance the state art of computer science and integrate research innovations in multi-disciplinary fields.
- To equip student / faculty with excellent teaching learning capabilities through advanced learning tools and technologies.
- To produce students with critical thinking and lifelong learning capabilities to apply their knowledge to uplift the living standards of the society.
- To produce students with enriched skill set, professional behavior, strong ethical values and leadership capabilities so as to work with commitment for the progress of the nation.

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

PROGRAMME EDUCATIONAL OBJECTIVES (PEO'S):

PEO1	Have successful careers in consulting firms, government, academic institutions, NGOs and Research and Development organization.
PEO2	Continue to enhance their acquired skills and qualifications though continues improvement Programs and Research and Development.
PEO3	Demonstrate their commitment for the welfare of the society through the application of the acquired knowledge for Societal Cause.

PROGRAMME OUTCOMES

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

At the end of the programme, the student shall be able to:

PO1 Apply the knowledge of mathematics, science and engineering to solve problems related to cyber security in various areas like Cryptography, digital Forensics, Biometric Security, and Web Security and so on.

PO2 Analyze complex security issues, make creative judgment and draw smart conclusions from Forensic evidences, identify security threats and vulnerabilities.

PO3 Use tools and techniques to test vulnerabilities using secure scanning.

PO4 Independently carry out research/investigation and development work to solve practical problems in Cyber crime and Investigations and Security issues.

PO5 Design solutions for complex technological problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

PO6 Develop and implement the security policies to meet the needs of an organization and the mandatory regulations by statutory bodies.

PO7 Apply ethical principles and commit to social issues, professional ethics, and responsibilities and norms of the engineering practice.

PO8 Gain the skills to communicate effectively with the social and technical organizations based on the subject matters and desertions.

PO9 Engage themselves in lifelong learning in the context of rapid technological Changes in cyber Security Specialization.

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

PO10 Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in Multidisciplinary environments.

PROGRAMME SPECIFIC OUTCOMES

PSO1 Define and implement the security policies to meet the needs of an organization and the mandatory regulations by statutory bodies.

PSO2 Identify the vulnerabilities and develop processes to mitigate security threats.

PSO3 Enhanced capability to develop computational tools and applications and improved skills to solve contemporary challenges

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

REVISED Bloom's Taxonomy Action Verbs

Definitions	I. Remembering	II. Understanding	III. Applying	IV. Analyzing	V. Evaluating	VI. Creating
Bloom's Definition	Exhibit memory of previously learned material by recalling facts, terms, basic concepts, and answers.	Demonstrate understanding of facts and ideas by organizing, comparing, translating, interpreting, giving descriptions, and stating main ideas.	Solve problems to new situations by applying acquired knowledge, facts, techniques and rules in a different way.	Examine and break information into parts by identifying motives or causes. Make inferences and find evidence to support generalizations.	Present and defend opinions by making judgments about information, validity of ideas, or quality of work based on a set of criteria.	Compile information together in a different way by combining elements in a new pattern or proposing alternative solutions.
Verbs	• Choose • Define • Find • How • Label • List • Match • Name • Omit • Recall • Relate • Select • Show • Spell • Tell • What • When • Where • Which • Who • Why	• Classify • Compare • Contrast • Demonstrate • Explain • Extend • Illustrate • Infer • Interpret • Outline • Relate • Rephrase • Show • Summarize • Translate	• Apply • Build • Choose • Construct • Develop • Experiment with • Identify • Interview • Make use of • Model • Organize • Plan • Select • Solve • Utilize	• Analyze • Assume • Categorize • Classify • Compare • Conclusion • Contrast • Discover • Dissect • Distinguish • Divide • Examine • Function • Inference • Inspect • List • Motive • Relationships • Simplify • Survey • Take part in • Test for • Theme	• Agree • Appraise • Assess • Award • Choose • Compare • Conclude • Criteria • Criticize • Decide • Deduct • Defend • Determine • Disprove • Estimate • Evaluate • Explain • Importance • Influence • Interpret • Judge • Justify • Mark • Measure • Opinion • Perceive • Prioritize • Prove • Rate • Recommend • Rule on • Select • Support • Value	• Adapt • Build • Change • Choose • Combine • Compile • Compose • Construct • Create • Delete • Design • Develop • Discuss • Elaborate • Estimate • Formulate • Happen • Imagine • Improve • Invent • Make up • Maximize • Minimize • Modify • Original • Originate • Plan • Predict • Propose • Solution • Solve • Suppose • Test • Theory

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M. Tech. (CY) I SEMESTER							
S.No	**Course Code**	**Courses**	**Category**	**L**	**T**	**P**	**C**
1	R19MCY1151	**Program Core-1** Principles of Cyber Security	PC	3	0	0	3
2	R19MCY1152	**Program Core-2** Applied Cryptography	PC	3	0	0	3
3	R19MCY1153	**Program Elective-1** 1. Operating Systems Administration and Security 2. Cyber Laws and Security Policies 3. Cloud and IoT Security	PE	3	0	0	3
4	R19MCY1154	**Program Elective-2** 1. Wireless Networks Security 2. Cyber Space Operations and Design 3. Database and Web Applications Security	PE	3	0	0	3
5	R19MCY1155	**Research Methodology and IPR**	CC			0	2
6	R19MCY1156	**Laboratory-1** Cyber Security Lab	LB	0	0	4	2
7	R19MCY1157	**Laboartory-2** Cryptography Lab	LB	0	0	4	2
8	R19MCY1158	**Audit Course-1** 1. English for Research Paper Writing 2. Disaster Management 3. Sanskrit for Technical Knowledge 4. Value Education	AC	2	0	0	0
Total Credits							18

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M. Tech. (CY) II SEMESTER							
S.No	**Course Code**	**Courses**	**Category**	**L**	**T**	**P**	**C**
1	R19MCY1251	**Program Core-3** Cyber Crime Investigation and Digital Forensics	PC	3	0	0	3
2	R19MCY1252	**Program Core-4** Ethical Hacking	PC	3	0	0	3
3	R19MCY1253	**Program Elective-3** 1. Software Vulnerability Analysis 2. Malware Analysis and Reverse Engineering 3. Application Threat Detection	PE	3	0	0	3
4	R19MCY1254	**Program Elective-4** 1. Biometric Security 2. Web Security 3. Firewall and VPN Security	PE	3	0	0	3
5	R19MCY1255	**Laboratory-3** Cyber Crime Investigation and Digital Forensics Lab	LB	0	0	4	2
6	R19MCY1256	**Laboartory-4** Ethical Hacking Lab	LB	0	0	4	2
7	R19MCY1257	**Mini Project with Seminar**	MP	2	0	0	2
8	R19MCY1258	**Audit Course-2** 1. Constitution of India 2. Pedagogy Studies 3. Stress Management by Yoga 4. Personality Development through Life Enlightenment Skills	AC	2	0	0	0
Total Credits							18

**Students are encouraged to go to Industrial Training/Internship for at least 2-3 months during semester break*

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M. Tech. (CY) III SEMESTER							
S.No	**Course Code**	**Courses**	**Category**	**L**	**T**	**P**	**C**
1	R19MCY2351	**Program Elective-5** 1. Cyber Security Governance 2. Principles of Secure Coding 3. Information System Audit 4. MOOCs-1 (NPTEL/SWAYAM)	PE	3	0	0	3
2	R19MCY2352	**Open Elective** 1. MOOCs (NPTEL/SWAYAM)-Any 12 Week Course on Engineering/ Management/ Mathematics offered by other than parent department 2. Course offered by other departments in the college	OE	3	0	0	3
3	R19MCY2353	**Dissertation-I/Industrial Project**		0	0	20	10
		Total Credits					16

*Students going for Industrial Project/Thesis will complete these courses through MOOCs

M. Tech. (CY) IV SEMESTER							
S.No	**Course Code**	**Courses**	**Category**	**L**	**T**	**P**	**C**
1	R19MCY2451	**Dissertation-II**		0	0	32	16
Total Credits							16

Open Electives offered by the Department of CSE for other Departments Students

1. Python Programming
2. Principles of Cyber Security
3. Internet of Things
4. Artificial Intelligence and Machine Learning

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M. Tech. (CY) I Semester

Principles of Cyber Security

Code: R19MCY1151

Course Objectives:

- To learn threats and risks within context of the cyber security architecture.
- Student should learn and Identify security tools and hardening techniques.
- To learn types of incidents including categories, responses and timelines for response.

Course Outcomes: At the end of the course, student will be able to

Course Outcomes		Knowledge Level (K)#
CO1	Apply cyber security architecture principles.	K3
CO2	Demonstrate the risk management processes and practices.	K2
CO3	Appraise cyber security incidents to apply appropriate response	K5
CO4	Distinguish system and application security threats and vulnerabilities.	K4
CO5	Identify security tools and hardening techniques	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												
CO4												
CO5												

(Please fill the above with Levels of Correlation, viz., L, M, H)

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

UNIT–I: Introduction to Cyber Security-Cyber security objectives, roles, differences between information security and cyber security, Cyber security principles-confidentiality, integrity, availability, authentication and non repudiation

UNIT–II: Information Security within Lifecycle Management-Lifecycle management landscape, Security architecture processes, Security architecture tools, Intermediate lifecycle management concepts, **Risks & Vulnerabilities-**Basics of risk management, Operational threat environments, Classes of attacks

UNIT–III: Incident Response-Incident categories, Incident response, Incident recovery, **Operational security protection**-Digital and data assets, ports and protocols, Protection technologies, Identity and access Management, configuration management

UNIT–IV: Threat Detection and Evaluation Monitoring-Vulnerability management, Security logs and alerts, Monitoring tools and appliances, **Analysis-**Network traffic analysis, packet capture and analysis

UNIT–V: Introduction to backdoor System and security-Introduction to metasploit, backdoor, demilitarized zone (DMZ), Digital signature, Brief study on Harding of operating system.

Text Books:

1. NASSCOM: Security Analyst Student Hand Book, Dec 2015
2. Information Security Management Principles, Updated Edition, David Alexander, Amanda Finch, David Sutton, BCS publishers, June 2013

Reference Books:

1. Cyber Security Fundamentals-Cyber Security, Network Security and Data Governance Security, 2nd Edition, ISACA Publishers, 2019

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M. Tech. (CY) I Semester

Applied Cryptography

Code: R19MCY1152

Course Objectives:

- Student learns the basic concepts of symmetric cryptography and simple encryption methods.
- An understanding of the RSA cryptosystem, the mathematics used in the system, and the ability to encrypt and decrypt clear text using the system.
- To learn the properties of message authentication codes and the ability to use hash functions to build a message authentication code.

Course Outcomes: At the end of the course, student will be able to

Course Outcomes		Knowledge Level (K)#
CO1	Demonstrate the basics of Cryptographic protocols and Stream Ciphers	K2
CO2	Explain the concepts of Public Key Encryption and Block Ciphers	K5
CO3	Demonstrate Number Theory for Symmetric and Asymmetric Ciphers and discuss various Ciphers	K2
CO4	Discuss Hashing Algorithms and Message Authentication Codes	K6
CO5	Elaborate Key-Exchange algorithms and Real world Implementations	K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												
CO4												
CO5												

(Please fill the above with Levels of Correlation, viz., L, M, H)

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

UNIT–I: Foundations, Protocol Building Blocks, Basic Protocols, Advanced Protocols - Zero-Knowledge Proofs, Zero-Knowledge Proofs of Identity, Blind Signatures, Identity-Based Public-Key Cryptography, Key Length, Key Management, Electronic Codebook Mode, Block Replay, Cipher Block Chaining Mode, Stream Ciphers, Self-Synchronizing Stream Ciphers, Cipher- Feedback Mode, Synchronous Stream Ciphers, Output-Feedback Mode, Counter Mode, Other Block-Cipher Modes, Choosing a Cipher Mode.

UNIT–II: Information Theory, Complexity Theory, Number Theory, Factoring, Prime Number Generation, Discrete Logarithms in a Finite Field, Data Encryption Standard (DES), IDEA, CAST, Blowfish, RC5, Double Encryption, Triple Encryption.

UNIT–III: Pseudo-Random-Sequence Generators and Stream Ciphers- Linear Congruential Generators, Linear Feedback Shift Registers, Stream Ciphers using LFSRs, RC4, Feedback with Carry Shift Registers, Stream Ciphers Using FCSRs, Nonlinear-Feedback Shift Registers, Other Stream Ciphers, One-Way Hash Functions- MD5, Secure Hash Algorithm (SHA), One Way Hash Functions Using Symmetric Block, Using Public Key Algorithms, Message Authentication Codes.

UNIT–IV: Public-Key Algorithms, Knapsack Algorithms, RSA, Rabinm ElGamal, Elliptic Curve Cryptosystems, Digital Signature Algorithm (DSA), DSA Variants, Gost Digital Signature Algorithm, Discrete Logarithm Signature Schemes, Ong-Schnorr-Shamir, Schnorr, Converting Identification Schemes to Signature Schemes.

UNIT–V: Diffie- Hellman, Station-to-Station Protocol, Multiple-Key Public-Key Cryptography, Subliminal Channel, Undeniable Digital Signatures, Designated Confirmer Signatures, Kerberos, Privacy-Enhanced Mail (PEM), Message Security Protocol (MSP), Pretty Good Privacy (PGP), Smart Cards, Public-Key Cryptography Standards (PKCS).

Text Books:

1. Cryptography and Network Security, 6th Edition, William Stallings, Pearson Education, March 2013
2. Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition, Bruce Schneier, John Wiley & Sons Inc, 1996

Reference Books:

1. Modern Cryptography Theory and Practice‖, 1st Edition, Wenbo Mao, Pearson Education, 2004
2. Cryptography and Network Security, 7th Edition, Atul Kahate, Tata McGrew Hill, 2003

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M. Tech. (CY) I Semester

Operating Systems Administration and Security

Code: R19MCY1153

Course Objectives:

- Students will learn and apply basic concepts and methodologies of System Administration and Security by building from the ground up a miniature corporate network.
- To know some basic security measures to take in system administration.
- To prepare for possible disasters, including an understanding of backup and restoration of file systems.

Course Outcomes: At the end of the course, student will be able to

Course Outcomes		Knowledge Level (K)#
CO1	Explain the important computer system resources and the role of operating system in their management policies and algorithms.	K2
CO2	Describe the concepts of Access control Fundamentals, Multics.	K4
CO3	Identify and assess current and anticipated security risks and vulnerabilities.	K3
CO4	Identify the security Techniques and apply the real time applications.	K3
CO5	Explain the role and responsibilities of a system administrator and Create and administer user accounts on both a Linux and Windows platform.	K5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												
CO4												
CO5												

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT–I: Overview of Operating Systems-Introduction, Computer system organization and architecture, Operating system structure and operations, Process Management, Memory Management, file systems management Protection and security, Scheduling Algorithms, Inter-process Communication(Text Book1)

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

UNIT-II: Operating Systems Protection: Protection Goals, Protection Threats, Access Control Matrix, Access Control Lists(ACL's), Capability Lists(C-lists), Protection systems, Lampson's access matrix, mandatory protection systems, Reference monitor, Secure operating system definition(Text Book 2)

UNIT–III: Operating System Security-Security Goals, Security Threats, Security Attacks- Trojan Horses, Viruses and Worms, Buffer Overflow attacks and Techniques, Formal Aspects of Security, Encryption- Attacks on Cryptographic Systems, Encryption Techniques, Authentication and Password Security, Intrusion detection, malware defences, UNIX and Windows security(Text Book 2)

UNIT–IV: System Administration: Security Basics, Securing the Server Itself, Maintenance and Recovery, Monitoring and Audit, Introduction to Linux Systems, Configuration Management, Log Auditing and Vulnerability Assessment.(Text Book 3)

UNIT–V: Linux Networking: Networking Technologies: DHCP, DNS, NFS/iSCSI, SMTP, SNMP, LAMP, Firewall/IDS/SSH, Securing Linux. **Case Studies**: Security and Protection-MULTICS, UNIX, LINUX and Windows, Windows and Linux Coexisting.(Text Book 4)

Text Books:

1. Operating System Concepts, 9th Edition, Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, Wiley Publication, 2008
2. Advanced Concepts in Operating Systems, 1st Edition, Mukesh Singhal and N. G. Shivaratri, McGraw- Hill, 2000

Reference Books:

1. Operating System: Internals and Design Principles, 7th Edition, William Stalling, Prentice Hall, 2012
2. An Introduction to Operating Systems: Concepts and practice, 4th Edition, Promod Chandra P Bhat, Prentice Hall of India, 2014
3. Linux System Administration, Tom Adelstein and Bill Lubanovic, 1st Edition, O'Reilly Media, Inc., 2009

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M. Tech. (CY) I Semester

Cyber Laws and Security Policies

Code: R19MCY1153

Course Objectives:

- To Enable Learner To Understand, Explore, And Acquire A Critical Understanding Cyber Law.
- Student learns and develops Competencies for Dealing with Frauds and Deceptions (Confidence Tricks, Scams) And Other Cyber Crimes For Example, Child Pornography Etc. That Are Taking Place Via The Internet.
- Student should learn security policies and procedures.

Course Outcomes: At the end of the course, student will be able to

Course Outcomes		Knowledge Level (K)#
CO1	Design the Social And Intellectual Property Issues Emerging From Cyberspace.	K6
CO2	Explain The Legal And Policy Developments In Various Countries To Regulate Cyberspace	K2
CO3	Develop The Understanding Of Relationship Between Commerce And Cyberspace.	K3
CO4	Determine in Depth Knowledge Of Information Technology Act And Legal Frame Work Of Right To Privacy, Data Security And Data Protection.	K5
CO5	Apply various Case Studies On Real Time Crimes.	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												
CO4												
CO5												

(Please fill the above with Levels of Correlation, viz., L, M, H)

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

UNIT–I: Introduction to Computer Security- Definition, Threats to security, Government requirements, Information Protection and Access Controls, Computer security efforts, Standards, Computer Security mandates and legislation, Privacy considerations, International security activity.

UNIT–II: Secure System Planning and administration- Introduction to the orange book, Security policy requirements, accountability, assurance and documentation requirements, and Network Security, The Redbook and Government network evaluations.

UNIT–III: Information security policies and procedures-Corporate policies- Tier 1, Tier 2 and Tier3 policies - process management-planning and preparation- developing policies- asset classification policy- developing standards.

UNIT–IV: Information security-fundamentals-Employee responsibilities- information classification- Information handling- Tools of information security- Information processing-secure program administration.

UNIT–V: Organizational and Human Security-Adoption of Information Security Management Standards, Human Factors in Security- Role of information security professionals, IT Act- Structure of IT Act, Common cyber crime scenarios and Applicability of Legal sections, Case studies as per selected IT Act sections.

Text Books:

1. Computer Security Basics (Paperback), 2nd Edition, Debby Russell and Sr. G.T Gangemi, O'Reilly Media, 2006
2. Information Security policies and procedures: A Practitioner's Reference‖, 2nd Edition, Thomas R. Peltier Prentice Hall, 2004

Reference Books:

1. Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions‖, Kenneth J. Knapp, IGI Global, 2009

Web References:

1. https://meity.gov.in/content/information-technology-act 2000

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

Cloud and IoT Security

Code: R19MCY1153

Course Objectives:

- Student learn and understand the advantages, challenges, security issues of cloud computing and interrelationships between cloud computing and big data.
- Student learns different Key components of Amazon Web Services, Cloud Backup and solutions.
- Student able to discuss the main threats and attacks on IoT products and services
- Be able to learn secure a connected IoT product from scratch.

Course Outcomes: At the end of the course, student will be able to

Course Outcomes		Knowledge Level (K)#
CO1	Analyze the Cloud Computing and the different Cloud services and deployment models	K4
CO2	Assessing the financial, technological, and organizational capacity of employer's for actively initiating and installing cloud-based applications.	K5
CO3	Explain how IOT can be used in different Industries.	K2
CO4	Identify how companies can plan for the future of technologies.	K3
CO5	Apply smart applications in real world.	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												
CO4												
CO5												

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT–I: Cloud Computing Fundamental-Cloud Computing definition, private, public and hybrid cloud. Cloud types; IaaS, PaaS, SaaS, Benefits and challenges of cloud computing, public vs private clouds, role of virtualization in enabling the cloud

UNIT–II: Cloud Applications-Development environments for service development; Amazon, Azure, Google App, Security management in the cloud – security

management standards- SaaS, PaaS, IaaS availability management- access control- Data security and storage in cloud

UNIT–III: The Internet of Things-An Overview of Internet of things, Internet of Things Technology, behind IoTs Sources of the IoTs, M2M Communication, Examples OF IoTs, Design Principles For Connected Devices Internet Connectivity Principles, Internet connectivity, Application Layer Protocols: HTTP, HTTPS, FTP, Telnet

UNIT–IV: IOT Design-Business Models for Business Processes in the Internet of Things, IoT/M2M systems LAYERS AND designs standardizations ,Modified OSI Stack for the IoT/M2M Systems, ETSI M2M domains and High-level capabilities ,Communication Technologies, Data Enrichment and Consolidation and Device Management Gateway Ease of designing and affordability

UNIT–V: IOT Security Issues- Secure constrained devices, Authorize and authenticate devices, Manage device updates, secure communication, Ensure data privacy and integrity, secure web, mobile, and cloud applications, Ensure high availability, Detect vulnerabilities and incidents, Manage vulnerabilities, Predict and preempt security issues.

Text Books:

1. Internet of Things: Architecture, Design Principles And Applications, 1st Edition, Rajkamal, McGraw Hill Higher Education, 2017
2. Internet of Things, 1st ed, A.Bahgya and V.Madisetti, University Press, 2015

Reference Books:

1. Enterprise Cloud Computing Technology Architecture Applications, 1st Edition, Gautam Shroff, Cambridge University Press, 2010
2. Cloud Computing, A Practical Approach, 1st Edition,Toby Velte, Anthony Velte, Robert Elsen peter, McGraw Hill, 2010
3. IOT Security Issues, 1st Edition, Alasdair Gilchrist, O'Reilly Publishers, 2017
4. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, 1st Edition, Tim Mather, Subra Kumara swamy, Shahed Latif, O'Reilly Publication, 2009

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M.Tech (CY) I Semester

Wireless Networks Security

Code: R19MCY1154

Course Objectives:

- To understand the concepts of network security threats, classify the threats and develop a security model to prevent, detect and recover from the attacks.
- Student should learn and Develop SSL or Firewall based solutions against security threats, employ access control techniques to the existing computer platforms such as UNIX and Windows NT.
- To learn and understand wireless technologies and apply real time applications.

Course Outcomes: At the end of the course, student will be able to

Course Outcomes		Knowledge Level (K)#
CO1	Explain the Threats in networks and provide Authentication to real time problems.	K2
CO2	Identify and investigate in-depth both early and contemporary threats to wireless networks security	K3
CO3	Analyze and determine for any organization the database security requirements and appropriate solutions	K4
CO4	Explain IP Security Issues and solve real time problems.	K5
CO5	Build the Basic specifications in Bluetooth Security.	K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												
CO4												
CO5												

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT-I: Introduction to Wireless: History of Wireless Technologies, History of Wireless Security, State of the Wireless Security Industry, 2001. **Wireless Threats:** Uncontrolled Terrain, Communications Jamming, DoS Jamming, Injections and Modifications of Data, Man-in-the-Middle (MITM) Attack, Rogue Client, Rogue Network Access Points, Attacker Equipment, Covert Wireless Channels, Roaming Issues, Cryptographic Threats

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

UNIT-II: Introduction to Wireless Security Protocols and Cryptography: Recovery the FUD, OSI Model, OSI Simplified, Internet Model, Wireless LAN Security Protocols, Cryptography, SSL/TLS, Secure Shell Protocols, Terminal Access and File Transfer, Port Forwarding a Word of Caution, Man-in-the-Middle of SSL/TLS and SSH, WTLS, WEP,802.1x, IP Security. **Security Considerations to Wireless Devices:** Wireless Device Security Issues, Physical Security, Information Leakage, Device Security Features, Application Security, Detailed Device Analysis, Laptops, Personal Digital Assistants (PDAS), Wireless Infrastructure

UNIT-III: Wireless Technologies and Applications: Introduction to Cellular Networks- FDMA, TDMA, CDMA, Spread Spectrum Primer, Analogy, TDMA Vs CDMA, PDC, Security Threats, GSM Security, GSM Algorithm Analysis. **Introduction to Wireless Data Networks:** Cellular Digital Packet Data (CDPD), CDPD Architecture, CDPD Security, Mobitex- Mobitex Architecture, Mobitex Security Architecture, General Packet Radio Service (GPRS)- GPRS Architecture, Security Issues, Introduction to the Wireless Application Protocol (WAP)- WAP Device, Gateway, Security Model

UNIT-IV: Wireless Standards and Technologies: Current and Future Technologies- Infrared, Radio, Spread Spectrum, OFDM, Current and Future Standards- IEEE 802, 802.11, The ABC's of 802.11, 802.11b, 802.11a, 802.11g, 802.11j, 802.11h and 5GPP, 802.11e, 802.11i, 802.11f, IEEE 802.15, IEEE 802.16, IEEE 802.1x, ETSI, HomeRF, Ultra wideband Radio (UWB). **Wireless Deployment Strategies:** Implementing Wireless LAN's- Security Considerations Common Wireless Network Applications, Enterprise Campus Designs, Wireless IST Design, Retail and Manufacturing Design, Small Office/Home Office Design (SOHO)

UNIT-V: Bluetooth Security: Basic Specifications, Piconets, Bluetooth Security Architecture, Scatternets, Security at the Baseband Layer and Link Layer, Frequency Hopping, Security Manager, Authentication, Encryption, Threats to Bluetooth Security

Text Books:

1. Wireless Security, Merritt Maxim and David Pollino, 1st Edition, Osborne/McGraw Hill, New Delhi, 2005
2. Wireless Security-Models, Threats and Solutions, 2nd Edition, Nichols and Lekka, Tata McGraw Hill, New Delhi, 2006

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

Reference Books:

1. Security in Computing, 5th Edition,Charles P. Fleeger, Prentice Hall, New Delhi, 2009
2. Cryptography & Network Security, Behrouz A.Forouzan, Tata McGraw Hill, India, New Delhi, 2009
3. Cryptography and Network Security, 4th Edition, William Stallings, Prentice Hall, New Delhi, 2006
4. Applied Cryptography, 2nd Edition, Bruce Schneier, John Wiley & Sons, New York, 2004

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M.Tech (CY) I Semester

Cyberspace Operations and Design

Code: R19MCY1154

Course Objectives:

- To understand the concept of full-spectrum cyberspace operations, the complexities of the cyberspace environment, as well as planning, organizing, and integrating cyberspace operations.
- Students will have a fundamental understanding of how to analyze, plan for, and execute cyberspace operations.
- To learn and understand Cyber Warriors and Warrior Corps.

Course Outcomes: At the end of the course, student will be able to

Course Outcomes		Knowledge Level (K)#
CO1	Explain the Concept of Cyberspace Environment and Design.	K2
CO2	Explain the Cyberspace Operational Approaches.	K2
CO3	Outline the cyberspace operation and integrate it with a Joint Operations plan.	K2
CO4	Build Cyber Warriors and Warrior Corps	K3
CO5	Designing Cyber Related Commands and Organizational structures.	K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												
CO4												
CO5												

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT–I: Understanding the Cyberspace Environment and Design- Cyberspace environment and its characteristics, developing a design approach, planning for cyberspace operation

UNIT–II: Cyberspace Operational Approaches- Foundational approaches that utilize cyberspace capabilities to support organizational missions, the pros and cons of the

different approaches, Cyberspace Operations- Network Operations (NETOPS), Defensive Cyberspace Operations (DCO), Offensive Cyberspace Operations (OCO), Defence and Diversity of Depth network design, Operational methodologies to conduct cyberspace operations

UNIT–III: Cyberspace Integration- Design a cyberspace operation and integrate it with a Joint Operations plan, Practice the presented methodologies in a practical application Experiment

UNIT–IV: Building Cyber Warriors and Warrior Corps- The warrior and warrior corps concept as applied to cyber organizations, the challenges of training and developing a cyber-workforce from senior leadership to the technical workforce

UNIT–V: Designing Cyber Related Commands- Mission statements, Essential tasks, Organizational structures, Tables of organizations, Training and Readiness for Cyber Related Commands- Mission Essential Tasks (METs), Developing the cyber workforce, Plan your own training programs within your organization

Text Books:

1. Introduction of Cyber Warfare: A Multidisciplinary Approach, 1st Edition, Paulo Shakarian et al., syngress, Elsevier 2013
2. Inside Cyber Warfare: Mapping the Cyber Underworld, 2nd Edition, Jeffery carr et al, O'Reilly Publication December 2012

Reference Books:

1. Cyber Warfare: Techniques, 2nd Edition, Tactics and Tools for Security Practitioners Syngress, Jason Andress et al., Elsevier 2013

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M.Tech (CY) I Semester

Database and Web Applications Security

Code: R19MCY1154

Course Objectives:

- To acquire knowledge on standard algorithms used to provide confidentiality, integrity and authenticity.
- To design security applications in the field of Information technology.
- To understand the fundamentals of database design, DB security and SQL extensions to security.
- To learn the basic concepts of Penetration testing.

Course Outcomes: At the end of the course, student will be able to

Course Outcomes		Knowledge Level (K)#
CO1	Explain threats, vulnerabilities and breaches to design database	K2
CO2	Discuss Relational Data Model and concurrency controls and locking, SQL extensions to security.	K6
CO3	Demonstrate the Browser security principles.	K2
CO4	Analyze the software centric security and mobile web browser security in real time applications	K4
CO5	Construct the penetrating testing workflows with examples.	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												
CO4												
CO5												

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT–I: Database security-Introduction includes threats, vulnerabilities and breaches, Basics of database design, DB security, concepts, approaches and challenges, types of access controls, Oracle VPD, Discretionary and Mandatory access control: Principles, applications and poly instantiation, Database inference problem, types of inference attacks, distributed database, security levels, SQL-injection: types and advanced concepts

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

UNIT–II: Relational Data Model- Security in relational data model, concurrency controls and locking, SQL extensions to security (oracle as an example), System R concepts, Context and control based access control, Hippocratic databases, Database watermarking, Database intrusion, Secure data outsourcing.

UNIT–III: Web application security-Basic principles and concepts, Authentication, Authorization, Browser security principles; XSS and CSRF, same origin policies, File security principles, Secure development and deployment methodologies, Web DB principles, OWASP – Top 10 -Detailed treatment, IoT security.

UNIT–IV: Mobile device security: Introduction, attack vector and models, hardware centric security aspects, SMS / MMS vulnerabilities, software centric security aspects, mobile web browser security, Application security: Concepts, CIA Triad, Hexad, types of cyber-attacks, Introduction to software development vulnerabilities, code analyzers – Static and dynamic analyzers.

UNIT–V: Penetration testing- Principles and concepts, PT work flows and examples, blind tests, ethical hacking techniques, synthetic transactions, interface testing and fuzzing, SDLC phases and security mandates.

Text Books:

1. Web Application Security, 1st Edition, A Beginners Guide, Bryan and Vincent, McGraw-Hill, 2011
2. Database Security, 1st Edition, Alfred Basta, Melissa Zgola, Course Technology, 2012

Reference Books:

1. Handbook of Database Security: Applications and Trends, Michael Gertz and Sushil Jajodia, Springer, 2008
2. Database and Applications Security, 1st Edition, Integrating Information Security and Data Management, Bhavani Thuraisingham, Auerbach Publications, 2005

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M.Tech (CY) I Semester

Research Methodology and IPR

Code: R19MCY1155

Course Objectives:

- Student able analyze the Effective literature studies approaches, analysis, Plagiarism, Research ethics.
- Student should able understand problem, Scope and objectives of research problem.
- To learn and understand Traditional knowledge Case Studies, IPR and IITs

Course Outcomes: At the end of the course, student will be able to

Course Outcomes		Knowledge Level (K)#
CO1	Demonstrate the research and its types	K2
CO2	Reviewing literature. Identifying and defining research problem.	K3
CO3	Explaining research design methods, sampling techniques	K5
CO4	Designing and development of measuring instruments, data collection and analysis methods	K6
CO5	Show the IPR protection provides an incentive to inventors for further research work and Investment in R & D, which leads to creation of new and better products, and in turn brings about, Economic growth and social benefits.	K1
CO6	Identify Research proposal, research report and evaluating research	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												
CO4												
CO5												
CO6												

(Please fill the above with Levels of Correlation, viz., L, M, H)

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

UNIT–I: Meaning of research problem, Sources of research problem, Criteria Characteristics of a good research problem, Errors in selecting a research problem, Scope and objectives of research problem, Approaches of investigation of solutions for research problem, data collection, analysis, interpretation, Necessary instrumentations

UNIT–II: Effective literature studies approaches, analysis, Plagiarism, Research ethics

UNIT–III: Effective technical writing, how to write report, Paper Developing a Research Proposal, Format of research proposal, a presentation and assessment by a review committee

UNIT–IV: Nature of Intellectual Property: Patents, Designs, Trade and Copyright. Process of Patenting and Development: technological research, innovation, patenting, development. International Scenario: International cooperation on Intellectual Property. Procedure for grants of patents, Patenting under PCT

UNIT–V: Patent Rights: Scope of Patent Rights. Licensing and transfer of technology. Patent information and databases. Geographical Indications

UNIT–VI: New Developments in IPR: Administration of Patent System. New developments in IPR; IPR of Biological Systems, Computer Software etc. Traditional knowledge Case Studies, IPR and IITs.

Text Book:

1. Research methodology: an introduction for science & engineering students,1st Edition, Stuart Melville, Wayne Goddard, 1996

Reference Books:

1. Research Methodology: A Step by Step Guide for beginners, 2nd Edition, Ranjit Kumar, 2011
2. Resisting Intellectual Property, 1st Edition, Halbert, Taylor & Francis Ltd., 2007

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M.Tech (CY) I Semester

Cyber Security Lab

Code: R19MCY1157

Course Objectives:

- Understand and apply vulnerabilities in web applications.
- Identify security tools and hardening techniques.

Course Outcomes: At the end of the course, student will be able to

Course Outcomes		Knowledge Level (K)#
CO1	Illustrate the knowledge of in-bound and out-bound rules in a client system.	K2
CO2	Identify security tools and hardening techniques.	K3
CO3	Design a backdoor on the target machine	K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												

(Please fill the above with Levels of Correlation, viz., L, M, H)

Experiment 1: Program to check vulnerabilities in web applications.

Experiment 2: Analysis of network traffic using packet capturing tools.

Experiment 3: Identify the open, close ports and protocols using tools.

Experiment 4: Identify the vulnerabilities in a network.

Experiment 5: Establishment of demilitarized zone.

Experiment 6: Hardening of operating system.

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

Experiment 7: Manually disabling unnecessary services and ports and locking down the ports.

Experiment 8: Implementation of in-bound and out-bound rules in a client system.

Experiment 9: Report bugs in any web application using tool.

Experiment 10: Program to implement metasploit in windows or Linux.

Experiment 11: Implementation of Incident response with tools.

Experiment 12: Identifying the vulnerable logs in windows system

Experiment 13: Generate digital certificates using tools.

Experiment 14: Establish a backdoor on the target machine via pivot points

Experiment 15: Implementation of patch Management in client system.

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M.Tech (CY) I Semester

Cryptography Lab

Code: R19MCY1156

Course Objectives:

- To learn basic understanding of cryptography, how it has evolved, and some key encryption techniques used today.
- To understand and implement encryption and decryption using Ceaser Cipher, Substitution Cipher, Hill Cipher.

Course Outcomes: At the end of the course, student will be able to

Course Outcomes		Knowledge Level (K)#
CO1	Apply the knowledge of symmetric cryptography to implement encryption and decryption using Ceaser Cipher, Substitution Cipher, Hill Cipher	K3
CO2	Demonstrate the different algorithms like DES, BlowFish, and Rijndael, encrypt the text "Hello world" using Blowfish Algorithm.	K2
CO3	Analyze and implement public key algorithms like RSA, Diffie-Hellman Key Exchange mechanism, the message digest of a text using the SHA-1 algorithm	K4

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												

(Please fill the above with Levels of Correlation, viz., L, M, H)

Experiment –1:
Write a Java program that contains a string (char pointer) with a value \Hello World'. The program should XOR each character in this string with 0 and displays the result.

Experiment –2:
Write a Java program that contains a string (char pointer) with a value \Hello World'. The program should AND or and XOR each character in this string with 127 and display the result.

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

Experiment –3:
Write a Java program to perform encryption and decryption using the following algorithms:

a) Ceaser Cipher
b) Substitution Cipher
c) Hill Cipher

Experiment –4:
Write a Java program to implement the Triple DES and AES algorithms.

Experiment –5:
Write a JAVA program to implement the BlowFish algorithm

Experiment -6:
Write a JAVA program to implement the Rijndael algorithm.

Experiment-7:
Using Java Cryptography, encrypt the text "Hello world" using BlowFish. Create your own key using Java keytool.

Experiment -8:
Implement MD-5 using Java

Experiment -9:
Write a Java program to implement RSA (2048 Key Length) Algorithm.

Experiment -10:
Implement the Diffie-Hellman Key Exchange mechanism using HTML and JavaScript. Consider the end user as one of the parties (Alice) and the JavaScript application as other party (bob).

Experiment -11:
Calculate the message digest of a text using the SHA-2 algorithm in JAVA.

Experiment-12:
Implement the Signature Scheme - Digital Signature Standard

Experiment-13:
Demonstrate how to provide secure data storage, secure data transmission and for creating digital signatures (GnuPG)

Experiment-14:
Implement encryption and decryption with openssl.

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

Experiment-15:
Calculate the message digest of a text using the SHA-1 algorithm in JAVA.

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M.Tech (CY) I Semester

English for Research Paper Writing

Code: R19MCY1158

Course Objectives:

- Understand that how to improve your writing skills and level of Readability
- Learn about what to write in each section
- Understand the skills needed when writing a Title

Course Outcomes: At the end of the course, student will be able to

Course Outcomes		Knowledge Level (K)#
CO1	How to improve your writing skills and level of readability	K1
CO2	Explain about what to write in each section	K3
CO3	Classify the skills needed when writing a Title	K2

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT–I: Planning and Preparation, Word Order, Breaking up long sentences, Structuring Paragraphs and Sentences, Being Concise and Removing Redundancy, Avoiding Ambiguity and Vagueness

UNIT–II: Clarifying Who Did What, Highlighting Your Findings, Hedging and Criticising, Paraphrasing and Plagiarism, Sections of a Paper, Abstracts Introduction

UNIT–III: Review of the Literature, Methods, Results, Discussion, Conclusions, The Final Check.

UNIT–IV: Key skills are needed when writing a Title, key skills are needed when writing an Abstract, key skills are needed when writing an Introduction, skills needed when writing a Review of the Literature

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

UNIT–V: Skills are needed when writing the Methods, skills needed when writing the Results, skills are needed when writing the Discussion, skills are needed when writing the Conclusions

UNIT–VI: Useful phrases, how to ensure paper is as good as it could possibly be the first- time submission.

Text Books:

1. Writing for Science, 0th Edition, Yale University Press, Goldbort R 2006
2. How to Write and Publish a Scientific Paper,7th Edition, Cambridge University Press, Day R 2006
3. Handbook of Writing for the Mathematical Sciences,2nd Edition, SIAM, Highman's book, Highman N 1998

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M.Tech (CY) I Semester

Disaster Management

Code: R19MCY1158

Course Objectives:

- Learn to demonstrate a critical understanding of key concepts in disaster risk reduction and humanitarian response.
- Critically evaluate disaster risk reduction and humanitarian response policy and practice from multiple perspectives.
- Develop an understanding of standards of humanitarian response and practical relevance in specific types of disasters and conflict situations.
- critically understand the strengths and weaknesses of disaster management approaches, planning and programming in different countries, particularly their home country or the countries they work in

Course Outcomes: At the end of the course, student will be able to

Course Outcomes		Knowledge Level (K)#
CO1	Demonstrate the critical understanding of key concepts in disaster risk reduction and humanitarian response.	K2
CO2	Evaluate disaster risk reduction and humanitarian response policy and practice from multiple perspectives.	K5
CO3	Develop an understanding of standards of humanitarian response and practical relevance in specific types of disasters and conflict situations.	K6
CO4	Analyze the strengths and weaknesses of disaster management approaches, planning and programming in different countries, particularly their home country or the countries they work in	K4
CO5	Describe disaster risk reduction and humanitarian response.	K2
CO6	Outline the disaster risk reduction and humanitarian response policy and practice from multiple perspectives.	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												
CO4												
CO5												

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

CO6												

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT–I: Introduction- Disaster- Definition, Factors and Significance; Difference between Hazard and Disaster; Natural and Manmade Disasters: Difference, Nature, Types and Magnitude.

UNIT–II: Repercussions Of Disasters And Hazards- Economic Damage, Loss of Human and Animal Life, Destruction of Ecosystem. Natural Disasters- Earthquakes, Volcanisms, Cyclones, Tsunamis, Floods, Droughts and Famines, Landslides and Avalanches, Man-made disaster: Nuclear Reactor Meltdown, Industrial Accidents, Oil Slicks and Spills, Outbreaks of Disease and Epidemics, War and Conflicts.

UNIT–III: Disaster Prone Areas In India- Study of Seismic Zones; Areas Prone to Floods and Droughts, Landslides and Avalanches, Areas Prone to Cyclonic and Coastal Hazards With Special Reference to Tsunami, Post-Disaster Diseases and Epidemics

UNIT–IV: Disaster Preparedness And Management- Preparedness: Monitoring of Phenomena Triggering A Disaster or Hazard; Evaluation of Risk: Application of Remote Sensing, Data from Meteorological and other Agencies, Media Reports: Governmental and Community Preparedness.

UNIT–V: Risk Assessment- Disaster Risk: Concept and Elements, Disaster Risk Reduction, Global and National Disaster Risk Situation. Techniques of Risk Assessment, Global Co-Operation in Risk Assessment and Warning, People's Participation in Risk Assessment, Strategies for Survival.

UNIT–VI: Disaster Mitigation- Meaning, Concept and Strategies of Disaster Mitigation, Emerging Trends in Mitigation, Structural Mitigation and Non-Structural Mitigation, Programs of Disaster Mitigation In India.

Text Books:

1. Disaster Management in India: Perspectives, issues and strategies¸ R. Nishith, Singh AK, New Royal book Company
2. Disaster Mitigation Experiences and Reflections, Sahni, New Title Edition , Pardeep Et. Al. (Eds.), Prentice Hall Of India, New Delhi
3. Disaster Administration and Management Text and Case Studies,1st Edition, Deep & Deep Publication Pvt. Ltd., Goel S. L., New Delhi

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M.Tech (CY) I Semester

Sanskrit for Technical Knowledge

Code: R19MCY1158

Course Objectives:

- To get a working knowledge in illustrious Sanskrit, the scientific language in the world
- Learning of Sanskrit to improve brain functioning
- Learning of Sanskrit to develop the logic in mathematics, science & other subjects
- enhancing the memory power
- The engineering scholars equipped with Sanskrit will be able to explore the
- Huge knowledge from ancient literature

Course Outcomes: At the end of the course, student will be able to

Course Outcomes		Knowledge Level (K)#
CO1	Demonstrate basic Sanskrit language	K2
CO2	Illustrate Ancient Sanskrit literature about science & technology	K2
CO3	Build a logical language will help to develop logic in students	K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT–I: Alphabets in Sanskrit, Past/Present/Future Tense.

UNIT–II: Simple Sentences forming in Sanskrit.

UNIT–III: Order of Sanskrit sentences, Introduction of roots in Sanskrit language.

UNIT–IV: Technical information about Sanskrit Literature.

UNIT–V: Technical concepts of Engineering-Electrical, Mechanical, Architecture,

Mathematics.

Text Books:

1. Abhyaspustakam – Dr.Vishwas, 1st Edition, Samskrita-Bharti Publication, New Delhi
2. Teach Yourself Sanskrit, Prathama Deeksha, VempatiKutumbshastri, Rashtriya Sanskrit Sansthanam, New Delhi Publication
3. India's Glorious Scientific Tradition,1st Edition, Suresh Soni, Ocean books (P) Ltd., New Delhi

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M.Tech (CY) I Semester

Value Education

Code: R19MCY1158

Course Objectives:

- Understand value of education and self- development
- Imbibe good values in students
- Let the should know about the importance of character

Course Outcomes: At the end of the course, student will be able to

Course Outcomes		Knowledge Level (K)#
CO1	Infer the knowledge of self-development	K2
CO2	Describe the importance of Human values	K2
CO3	Developing the overall personality	K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT–I: Values and self-development- Social values and individual attitudes. Work ethics, Indian vision of humanism. Moral and non- moral valuation, Standards and principles, Value judgments

UNIT–II: Importance of cultivation of values- Sense of duty, Devotion, Self-reliance, Confidence, Concentration. Truthfulness, Cleanliness, Honesty, Humanity, Power of faith, National Unity, Patriotism. Love for nature, Discipline.

UNIT–III: Personality and Behaviour Development-Soul and Scientific attitude, Positive Thinking, Integrity and discipline, Punctuality, Love and Kindness, Avoid fault Thinking.

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

UNIT – IV: Free from anger, Dignity of labour- Universal brotherhood and religious tolerance, True friendship, Happiness Vs suffering, love for truth, Aware of self-destructive habits, Association and Cooperation, Doing best for saving nature.

UNIT – V: Character and Competence- Holy books vs Blind faith, Self-management and Good health, Science of reincarnation, Equality, Nonviolence, Humility, Role of Women, All religions and same message, Mind your Mind, Self-control, Honesty, Studying effectively.

Text Books:

1. Values and Ethics for organizations Theory and practice, Latest Edition, Chakroborty, S.K., Oxford University Press, New Delhi

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M. Tech (CY) II Semester

Cyber Crime Investigation and Digital Forensics

Code: R19MCY1251

Course Objectives:

- Able to identify security risks and take preventive steps
- To understand the forensics fundamentals.
- To understand the evidence capturing process.
- To understand the preservation of digital evidence.

Course Outcomes: At the end of the course, student will be able to

	Course Outcomes	Knowledge Level (K)#
CO1	Explain the computer forensics fundamentals.	K2
CO2	Describe the types of computer forensics technology	K3
CO3	Analyze various computer forensics systems.	K4
CO4	Illustrate the methods for data recovery, evidence collection and data seizure.	K2
CO5	Identify the Role of CERT-In Security	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												
CO4												
CO5												

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT–I: Introduction- Introduction and Overview of Cyber Crime, Nature and Scope of Cyber Crime, Types of Cyber Crime: Social Engineering, Categories of Cyber Crime, Property Cyber Crime.

UNIT–II: Cyber Crime Issues- Unauthorized Access to Computers, Computer Intrusions, White collar Crimes, Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Pornography, Software Piracy, Intellectual Property, Mail Bombs, Exploitation ,Stalking and Obscenity in Internet, Digital laws and legislation, Law Enforcement Roles and Responses.

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

UNIT–III: Investigation- Introduction to Cyber Crime Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Hands on Case Studies. Encryption and Decryption Methods, Search and Seizure of Computers, Recovering Deleted Evidences, Password Cracking.

UNIT–IV: Digital Forensics- Introduction to Digital Forensics, Forensic Software and Hardware, Analysis and Advanced Tools, Forensic Technology and Practices, Forensic Ballistics and Photography, Face, Iris and Fingerprint Recognition, Audio Video Analysis, Windows System Forensics, Linux System Forensics, Network Forensics.

UNIT–V: Role of CRET-In Cyber Security- Computer Security Incident Response (Reactive) – Computer Security Incident Prevention (Proactive) – Security Quality Management Services, CERT-In Security Guidelines- Web server, database server, Intrusion Detection system, Routers, Standard alone system, networked System, IT Security polices for government and critical sector organizations.

Textbook:

1. Digital Forensics Basics: A Practical Guide Using Windows OS Paperback, 1st Edition, February 26, 2019

Reference Books:

1. Computer Forensics and Investigations, Nelsonm Phillips and Enfinger Steuart, 5th Edition, Cengage Learning, New Delhi, 2009
2. Incident Response and Computer Forensics, Kevin Mandia, Chris Prosise, Matt Pepe, 1st Edition, Tata McGraw-Hill, New Delhi, 2006
3. Software Forensics, Robert M Slade, Tata McGraw - Hill, New Delhi, 2005

Web Reference:

1. CERT-In Guidelines-http://www.cert-in.org.in/

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M. Tech (CY) II Semester

Ethical Hacking

Code: R19MCY1252

Course Objectives:

- The aim of the course is to introduce the methodologies and framework of ethical hacking for enhancing the security.
- The course includes-Impacts of Hacking; Types of Hackers; Information Security Models, Information Security Program, Business Perspective, Planning a Controlled Attack
- Framework of Steps (Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Deliverable and Integration)

Course Outcomes: At the end of the course, student will be able to

	Course Outcomes	Knowledge Level (K)#
CO1	Explain the concepts related to malware, hardware and software vulnerabilities and their causes	K2
CO2	Determine the applicable laws, legal issues and ethical issues regarding computer crime.	K4
CO3	Explain the business need for security, threats, attacks, top ten security vulnerabilities, and secure software development.	K2
CO4	Demonstrate systematic understanding of the concepts of security at the level of policy and strategy in a computer system	K2
CO5	Evaluate security techniques used to protect system and user data	K5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												
CO4												
CO5												

(Please fill the above with Levels of Correlation, viz., L, M, H)

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

UNIT–I: Introduction to Hacking- Important Terminologies, Types of Ethical Hacking, phases of Ethical Hacking, Categories of Penetration Testing.

UNIT–II: Phases of Ethical Hacking I- Information Gathering Techniques, Target Enumeration and Port Scanning Techniques, Vulnerability Assessment.

UNIT–III: Phases of Ethical Hacking II-Network Sniffing, Exploitation, Remote Exploitation, Client Exploitation, Web Exploitation.

UNIT–IV: System Hacking- Password cracking techniques- Key loggers, Escalating privileges, Hiding Files, Double Encoding, Steganography technologies and its Countermeasures. Active and passive sniffing ARP Poisoning, MAC Flooding, SQL Injection, Error based, Union-based, Time-based, Blind SQL, Out-of-band, Injection Prevention Techniques.

UNIT–V: Wireless Hacking- Wi-Fi Authentication Modes, Bypassing WLAN Authentication, Types of Wireless Encryption, WLAN Encryption Flaws, AP Attack, Attacks on the WLAN Infrastructure, DoS-Layer1, Layer2, Layer 3, DDoS Attack, Client Mis-association, Wireless Hacking Methodology, Wireless Traffic Analysis.

Text book:

1. Hacking: Be a Hacker with Ethics,2nd Edition, Harsh Bothra, Khanna Publications, 2019
2. Ethical Hacking and Penetration Testing Guide,1st Edition, Rafay Baloch, 2014

Reference Books:

1. Kali Linux Wireless Penetration Testing Beginner's Guide, Vivek Ramachandran, 1st Edition, Cameron Buchanan, Packt Publishing, 2015
2. SQL Injection Attacks and Defense, 1st Edition, Justin Clarke-Salt, Syngress Publication, 2012
3. Mastering Modern Web Penetration Testing, Prakhar Prasad, Packt Publishing, October 2016

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M.Tech (CY) II Semester

Software Vulnerability Analysis

Code: R19MCY1253

Course Objectives:

- This course provides the user to know the software vulnerabilities in the real software world.
- Different application level security
- Able to find the malicious code actions and different protection techniques.

Course Outcomes: At the end of the course, student will be able to

	Course Outcomes	Knowledge Level (K)#
CO1	Contrast the basic concepts of security & Authentication	K2
CO2	Illustrate the Malicious Code in software applications	K2
CO3	Analyze and apply Access Control & Physical Protection to the UNIX and Windows operating system	K4
CO4	Explain the concepts of OSI Model, Sockets	K2
CO5	Explain the concepts of Counter Measures	K5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												
CO4												
CO5												

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT-I: Introduction to security & Authentication- Software Security Dealing with Widespread Security Failures, Bugtraq, CERT Advisories, RISKS Digest, Technical Trends Affecting Software Security, The ileitis, Beyond Reliability, Penetrate and Patch, On Art and Engineering, Security Goals, Prevention, Traceability and Auditing, Monitoring, Privacy and Confidentiality, Multilevel Security.

UNIT-II: Application Security & Malicious Code-Managing Software Security Risk: An Overview Of Software Risk Management For Security, The Role Of Security Personnel, Software Security Personnel In The Life Cycle, Deriving Requirements, Risk

Assessment, Software Risk Management, Architectural Risk Analysis, Risk-Based Security Testing, Security Requirements, Security Operations.

UNIT-III: Access Control & Physical Protection- The UNIX Access Control Model, How UNIX and Windows Exploits, Modifying File Attributes, Modifying Ownership, The unmask, The Programmatic Interface, Setuid Programming, Access Control In Windows NT, Compartmentalization, Fine-Grained Privileges. Buffer Overflow & Root kits: Buffer Overflows As Security Problems, Defending Against Buffer Overflow.

UNIT-IV: Network Security& Intrusion- OSI Model, Sockets-Functions, Addresses, Network Byte Order, Internet Address Conversion, Simple Server and Web Clients, Tiny web Server. Peeling Back the Lower Layers, Network Sniffing, Raw Socket Sniffer, libpcap Sniffer, Decoding the Layers, Active Sniffing, Denial of Service, SYN Flooding, The Ping of Death, Teardrop, Ping Flooding, Amplification Attacks, Distributed DoS Flooding.

UNIT-V: Counter Measures- Detection of System Daemons, Crash Course in Signals, Tiny web Daemon, Tools of the Trade, tiny web Exploit Tool, Log Files, Log less Exploitation, Socket Reuse, Payload Smuggling, String Encoding, Buffer Restrictions, Polymorphic Printable ASCII Shell code. Hardening Countermeasures, Non executable Stack, ret2libc, Returning into system() Randomized Stack Space, Investigations with BASH and GDB, Bouncing Off Linux gate. Applied Knowledge, First Attempts, Paying the Odds.

Text Books:

1. Building Secure Software: How to Avoid Security Problems the Right Way, John Viega & Gary McGraw, Addison-Wesley Professional Computing Series, 1st Edition, 2019
2. Software Security: Building Security In, Gary McGraw, Addison-Wesley Professional Computing Series, 2006

Reference Books:

1. 19 Deadly Sins of Software Security: Programming Flaws and How to Fix Them (Security One-off), Michael Howard, David LeBlanc, John Viega, Addison-Wesley Professional Computing Series, 2005
2. Hacking: The Art of Exploitation, 2nd Edition, Jon Erickson, No Starch Press, San Fransico, 2008
3. Software Security, Theory Programming and Practice, Richard Sinn, Cengage Learning, 2015

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M.Tech (CY) II Semester

Malware Analysis and Reverse Engineering

Code: R19MCY1253

Course Objectives:

- To understand the purpose of computer infection program.
- To implement the covert channel and mechanisms.
- To test and exploit various malware in open source environment.
- To analyze and design the famous virus and worms.
- Understand the Reverse Engineering (RE) Methodology
- Disassemble products and specify the interactions between its subsystems and their functionality

Course Outcomes: At the end of the course, student will be able to

	Course Outcomes	**Knowledge Level (K)#**
CO1	Explain the characteristics of Malware and its effects on Computing systems.	K2
CO2	Predict the given system scenario using the appropriate tools to Identify the vulnerabilities and to perform Malware analysis.	K6
CO3	Analyze the given Portable Executable and Non-Portable Executable files using Static and dynamic analysis techniques.	K4
CO4	Demonstrate the Malware functionalities.	K2
CO5	Apply anti-reverse engineering in different Applications.	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**
CO1												
CO2												
CO3												
CO4												
CO5												

(Please fill the above with Levels of Correlation, viz., L, M, H)

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

UNIT–I: Malware Basics-Fundamentals of Malware Analysis (MA), MA tools and techniques, Static Malware Analysis, Dynamic Malware Analysis, Recent Malware Case Studies.

UNIT–II: Basic Analysis-Antivirus Scanning, x86 Disassembly, Hashing, Finding Strings, Packed Malware, PE File Format, Linked Libraries & Functions, PE Header File &Section.

UNIT–III: Advanced Static & Dynamic Analysis-IDA Pro, Recognizing C code constructs, Analyzing malicious windows program, Debugging, OllyDbg, Kernel Debugging with WinDbg, Malware Focused Network Signatures.

UNIT–IV: Malware Functionalities- Malware Behavior, Covert Malware Launch, Data Encoding, Shell code Analysis.

UNIT–V: Reverse Engineering Malware (REM)- REM Methodology, Resources for Reverse-Engineering Malware (REM) Understanding Malware Threats, Malware indicators, Malware Classification, Examining ClamAV Signatures, Creating Custom ClamAV Databases

Text books:

1. Computer Viruses: from theory to applications, Erci Filiol, 1st edition, Springer, 2005

Reference Books:

1. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, Michael Sikorski, Andrew Honig, publisher William Pollock, 2012

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M.Tech (CY) II Semester

Application Threat Detection

Code: R19MCY1253

Course Objectives:

- Can detect threats to any web app.
- Able to perform various Input Injection Attacks.
- Able to provide countermeasures against various input injection attacks.

Course Outcomes: At the end of the course, student will be able to

Course Outcomes		Knowledge Level (K)#
CO1	Explain Hacking Web Apps and Profiling	K5
CO2	Illustrate to provide Authentication to the web application.	K2
CO3	Develop Penetration Testing and implement Input Injection Attacks.	K3
CO4	Identify the basic fundamentals of Metasploit	K3
CO5	Apply knowledge on Capturing User Input and Abusing UI Expectations	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												
CO4												
CO5												

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT–I: Hacking Web Apps and Profiling-Web Application Hacking: GUI web Hacking, URI Hacking, Methods Headers and Body, Resources, The Web Client and HTML, Other Protocols, How & Why Web Apps attack, Infrastructure Profiling: Foot printing and Scanning, Basic Banner Grabbing, Advanced HTTP Fingerprinting, Infrastructure Intermediaries. Application Profiling: Manual Inspection, Search Tools for Profiling, Automated Web Crawling, General Countermeasures.

UNIT–II: Bypassing and Attacking Web Authentication-Web Authentication Threats: Username/password Threats, Password Guessing and its Countermeasures, Eavesdropping attacks and its Countermeasures, Forms-based Authentication attacks

and its countermeasures. Stronger web Authentication, Web Authentication Services. Bypassing Authentication: Token Replay, Cross-site Request Forgery, and Identity Management.

UNIT–III: Penetration Testing and Input Injection Attacks- Where to find Attack vectors, Common Input Injection Attacks: Buffer Overflow, Canonicalization and its countermeasures, Advanced Directory Traversal, Navigating Without Directory Listing, HTML Injection: XSS, Embedded scripts, Cookies and Predefined Headers, Counter countermeasures. SQL Injection: SUB Queries, UNION, SQL Injection countermeasures, XPATH Injection and its countermeasures, LDAP Injection.

UNIT–IV: Metasploit-Basics of Penetration Testing: The Phase of PTES, Types of Penetration Tests. Metasploit: Introduction, Metasploit Basics: Terminology, Metasploit Interfaces, Metasploit Utilities. Intelligence Gathering: Passive Information Gathering, Active Information Gathering, Target Scanning. Vulnerability Scanning: Basic Vulnerability Scan, Scanning with scanning tools, Using Scan Results for Autopwning.

UNIT–V: Attacking Users-Defacing Content, Capturing User Input: Using Focus Event, Using Keyboard Events, Using Mouse and Pointer Events, Using Form Events, Social Engineering: Using TabNabbing, Abusing UI Expectations: Using Fake Login Prompts, Pretty Theft, Gmail Phishing

Text Books:

1. Hacking Exposed Web Application, 3rd Edition by Joel Scambray, Vincent Liu, Caleb Sima, 2010
2. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition , Dafydd Stuttard, Marcus Pinto Wiley Publication, 2011
3. Metasploit - The Penetration Tester's Guide, 1st Edition, David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni – No Starch Press Publication, 2011

Reference Books:

1. The Browser Hacker’s Handbook by Wade Alcorn, 1st Edition, Christian Frichot and Michele Orru, Wiley Publication, 2014
2. Web Penetration Testing with Kali Linux, 3rd Edition, Joseph Muniz, AamirLakhan, Packt Publication, 2013

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M.Tech (CY) II Semester

Biometric Security

Code: R19MCY1254

Course Objectives:

- Describe the principles of the three core biometric modalities (face, fingerprint and iris), and know how to deploy them in authentication scenarios
- Organize and conduct biometric data collections, and apply biometric databases in system evaluation
- Calculate distributions of within- and between-class matching scores, and calculate various error estimates based on these distributions
- Identify the privacy and security concerns surrounding biometric systems, and know how to address them in such a way that balances both
- Recognize differences between algorithm design and systems engineering in biometrics
- Deploy statistical methods in biometric system evaluation
- Itemize the most up-to-date examples of real biometric applications in human authentication.

Course Outcomes: At the end of the course, student will be able to

	Course Outcomes	**Knowledge Level (K)#**
CO1	Demonstrate knowledge of the basic physical and biological science and engineering principles underlying biometric systems	K2
CO2	Analyze biometric systems at the component level and be able to analyze and design basic biometric system applications	K4
CO3	Illustrate to work effectively in teams and express their work and ideas orally and in writing	K2
CO4	Identify the sociological and acceptance issues associated with the design and implementation of biometric systems	K3
CO5	Elaborate various Biometric security issues in real world applications	K6

#Based on suggested Revised BTL

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												
CO4												
CO5												

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT–I: Biometrics- Introduction, benefits of biometrics over traditional authentication systems, benefits of biometrics in identification systems, selecting a biometric for a system, Applications, Key biometric terms and processes, biometric matching methods, Accuracy in biometric systems

UNIT–II: Physiological Biometric Technologies- Fingerprints, Technical description, characteristics, Competing technologies, strengths, weaknesses, deployment, Facial scan, Technical description, characteristics, weaknesses, deployment, Iris scan, Technical description, characteristics, strength, weaknesses, deployment

UNIT–III: Physiological Biometric Technologies- Hand Biometric: Palm Print, Vein Pattern, Signature and Hand Writing Technology-Technical description, characteristics, strengths, weaknesses and deployment.

UNIT–IV: Behavioural Biometric Technologies- Voice Recognition and Key stroke dynamics: Introduction, working, strengths and weaknesses, Voice Recognition Applications, Understanding Voice Recognition, Choice of Features, Speaker modeling, Pattern Matching, Key Stroke Dynamics, Active and Passive Biometrics.

UNIT – V: Multi biometrics and multi factor biometrics- two-factor authentication with passwords, tickets and tokens, executive decision, implementation plan, Securing Biometric Template- Cancelable Biometrics, Authentication, Security Analysis.

Text Books:

1. A Privacy Enhancing Biometric, Chuck Wilson, Vein pattern recognition, CRC press, 1st Edition, 2010
2. Biometrics: Identity Verification in a Network, 1st Edition, Samir Nanavathi, Michel Thieme, and Raj Nanavathi, Wiley Eastern, 2002
3. Implementing Biometric Security, 1st Edition, John Chirillo and Scott Blaul Wiley Eastern Publication, 2005

Reference Books:

1. Security, Risk and the Biometric State: Governing Borders and Bodies, 1st Edition, Benjamin Muller, Routledge, 2010
2. Handbook of Biometrics, Jain, Anil K.; Flynn, Patrick; Ross, Arun A. (Eds.), Springer, 2008
3. Handbook of Biometrics, Anil K. Jain, Patrick Flynn, Arun A. Ross, Springer, 2007
4. Biometrics for Network Security, 1st Edition, John Berger, Prentice Hall, 2004

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M.Tech (CY) II Semester

Web Security

Code: R19MCY1254

Course Objectives:

- Underlying security principles of the web
- Overview of concrete threats against web applications
- Insights into common attacks and countermeasures
- Current best practices for secure web applications

Course Outcomes: At the end of the course, student will be able to

	Course Outcomes	Knowledge Level (K)#
CO1	Demonstrate security concepts, security professional roles, and security resources in the context of systems and security development life cycle	K2
CO2	Justify applicable laws, legal issues and ethical issues regarding computer crime	K5
CO3	Explain the business need for security, threats, attacks, top ten security vulnerabilities, and secure software development	K2
CO4	Apply information security policies, standards and practices, the information security blueprint	K3
CO5	Analyze and describe security requirements for typical web application scenario	K4

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												
CO4												
CO5												

(Please fill the above with Levels of Correlation, viz., L, M, H)

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

UNIT–I: Introduction-A web security forensic lesson, Web languages, Introduction to different web attacks, Overview of N-tier web applications, Web Servers-Apache, IIS.

UNIT-II: Securing the Communication Channel- Understanding the dangers of an insecure communication channel. Practical advice on deploying HTTPS, and dealing with the impact on your application, Insights into the latest evolutions for HTTPS deployments.

UNIT–III: Web Hacking Basics- HTTP & HTTPS URL, Web under the Cover Overview of Java security Reading the HTML source, Applet Security Servlets Security Symmetric and Asymmetric Encryptions, Network security Basics, Firewalls & IDS.

UNIT–IV: Securely Handling Untrusted Data-Investigation of injection attacks over time, Understanding the cause behind both server-side and client-side injection attacks, Execution of common injection attacks, and implementation of various defenses.

UNIT–V: Preventing Unauthorized Access-Understanding the interplay between authentication, authorization and session management. Practical ways to secure the authentication process prevent authorization bypasses and harden session management mechanisms, Securing Large Applications, Cyber Graffiti.

Text Books:

1. Web Hacking: Attacks and Defense, Latest Edition , McClure, Stuart, Saumil Shah, and Shreeraj Shah, Addison Wesley, 2003
2. Professional Java Security, 1.3 Edition, Garms, Jess and Daniel Somerfield, Wrox, 2001

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M.Tech (CY) II Semester

Firewall and VPN Security

Code: R19MCY1254

Course Objectives:

- Identify and assess current and anticipated security risks and vulnerabilities
- Develop a network security plan and policies
- Establish a VPN to allow IPSec remote access traffic
- Monitor, evaluate and test security conditions and environment
- Develop critical situation contingency plans and disaster recovery plan
- Implement/test contingency and backup plans and coordinate with stakeholders
- Monitor, report and resolve security problems

Course Outcomes: At the end of the course, student will be able to

	Course Outcomes	**Knowledge Level (K)#**
CO1	To show the fundamental knowledge of Firewalls and it types	K2
CO2	Construct a VPN to allow Remote Access, Hashing, connections with Cryptography and VPN Authorization	K3
CO3	Elaborate the knowledge of depths of Firewalls, Interpreting firewall logs, alerts, Intrusion and Detection	K6
CO4	Infer the design of Control Systems of SCAD, DCS, PLC's and ICS's	K2
CO5	Evaluate the SCADA protocols like RTU, TCP/IP, DNP3, OPC,DA/HAD	K5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**
CO1												
CO2												
CO3												
CO4												
CO5												

(Please fill the above with Levels of Correlation, viz., L, M, H)

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

UNIT–I: Firewall Fundamentals- Introduction, Types of Firewalls, Ingress and Egress Filtering, Types of Filtering, Network Address Translation (NAT), Application Proxy, Circuit Proxy, Content Filtering, Software versus Hardware Firewalls, IPv4 versus IPv6 Firewalls, Dual-Homed and Triple-Homed Firewalls, Placement of Firewalls.

UNIT– II: VPN Fundamentals- VPN Deployment Models and Architecture, Edge Router, Corporate Firewall, VPN Appliance, Remote Access, Site-to-Site, Host-to-Host, Extranet Access, Tunnel versus Transport Mode, The Relationship Between Encryption and VPNs, Establishing VPN Connections with Cryptography, VPN Authorization.

UNIT–III: Exploring the Depths of Firewalls- Firewall Rules, Authentication and Authorization, Monitoring and Logging, Understanding and Interpreting Firewall Logs and Alerts, Intrusion Detection, Limitations of Firewalls, Downside of Encryption with Firewalls, Firewall Enhancements and Management Interfaces.

UNIT–IV: Overview of Industrial Control Systems- Overview of SCADA, DCS, and PLCs, ICS Operation, Key ICS Components, Control Components, Network Components, SCADA Systems, Distributed Control Systems, Programmable Logic Controllers, Industrial Sectors and Their Interdependencies.

UNIT–V: SCADA Protocols- Modbus RTU, Modbus TCP/IP, DNP3, DNP3 TCP/IP, OPC, DA/HAD, SCADA protocol fuzzing, Finding Vulnerabilities in HMI: software-Buffer Overflows, Shell code. Previous attacks Analysis- Stuxnet, Duqu.

Text Books:

1. Network Security, Firewalls, and VPN's, 1st Edition, Michael Stewart, Jones & Bartlett Learning, September 2010
2. Cyber security for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS, T. Macaulay and B. L. Singer, Auerbach Publications, 2011

Reference Books:

1. Critical Infrastructure Protection Information Infrastructure Models, Analysis, and Defense, J. Lopez, R. Setola, and S. Wolthusen, Springer-Verlag Berlin Heidelberg, 2012
2. Handbook of SCADA/Control Systems Security, 1st Edition, Robert Radvanovsky and Jacob Brodsky, CRC Press, 2013
3. Industrial Cloud-Based Cyber-Physical Systems, A.W. Colombo, T. Bangemann, S. Karnouskos, S. Delsing, P. Stluka, R. Harrison, et al., Springer International Publishing, 2014
4. Practical SCADA for Industry, D. Bailey, Burlington, MA: Newnes, 2003

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M.Tech (CY) II Semester

Cyber Crime Investigation and Digital Forensics Lab

Code: R19MCY1255

Course Objectives:

- Investigate cybercrime and collect evidences
- Able to use knowledge of forensic tools and software
- To understand the preservation of digital evidence.
- To learn about stenography Perceptual models

Course Outcomes: At the end of the course, student will be able to

	Course Outcomes	**Knowledge Level (K)#**
CO1	Identify the importance of a systematic procedure for investigation of data found on digital storage media that might provide evidence of wrong-doing.	K3
CO2	Construct the file system storage mechanisms of two common desktop opera ting systems and forensics tools used in data analysis.	K6
CO3	List and Implement all running processes, network connections from a memory image and find whether a firewall is set by analyzing a memory image.	K4
CO4	Design and develop live incident response on a system, View all browser history and List out all established network connections in a computer (Hint: Triage Incident Response).	K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**
CO1												
CO2												
CO3												
CO4												

(Please fill the above with Levels of Correlation, viz., L, M, H)

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

Experiment- 1

Evidence Collection

a) Linux: Capturing RAM dump using fmem
   https://github.com/NateBrune/fmem
   i) dcfldd if=/dev/fmem of=memory.dump hash=sha256
      sha256log=memory.dump.sha256 bs=1MB count=1000

b) Linux: Capturing Disk using dfldd
   https://www.obsidianforensics.com/blog/imaging-using-dcfldd
   i) dcfldd if=/dev/sdb1 of=/media/disk/test_image.dd hash=md5,
      sha1hashlog=/media/disk/hashlog.txt

Experiment- 2

a) Windows: Capture RAM dump of a windows system
   a. Hint: FTK Imager or RAM Capture

b) Windows: Capture Disk Image of a windows system

Hint: FTK Imager

Experiment- 3

Disk Analysis

i) List all files in a directory from a disk image
   a. FTK Imager
ii) Export a particular file from a disk image
   a. FTK Imager
iii) Recover a deleted file from a disk image

Hint: FTK Imager

Experiment- 4

Memory Analysis

1. List all running processes from a memory image
2. List all network connections from a memory image
3. Find out whether a firewall is set by analyzing a memory image

Hint: volatility

Experiment- 5

Live Incident Response

1. Perform live incident response on a system
2. View all browser history in a computer
3. List out all established network connections in a computer
   Hint: Triage Incident Response

Experiment – 6: Implement E-Mail Tracking and Email Investigation

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

Experiment – 7: Implement video Analytics for a live video

Experiment – 8: Analysis on different Malware Working

Experiment - 9: Work on Mail Bombs &SMS bombs

Experiment – 10: Implement a case on windows and Linux forensics

Experiment – 11: Implement a case on network Forensic

Experiment – 12: Work on different types of vulnerabilities

Experiment-13: Implement a case on Mobile Forensics

Experiment -14: Develop a Evidence and Preparation and Documentation

Experiment -15: Using kgbkeylogger tool record or generate a document what a user working on system

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M. Tech (CY) II Semester

Ethical Hacking Lab

Code: R19MCY1256

Course Objectives:

- Practice the objectives presented in the EC-Council's Certified Ethical Hacker certification
- Exploit networks like an attacker and discover how protect the system from them
- Determine the type of attack used and pinpoint exploit code in network traffic
- Leverage network and discovery mapping tools to identify systems on a network

Course Outcomes: At the end of the course, student will be able to

	Course Outcomes	Knowledge Level (K)#
CO1	Build the knowledge on Nmap, hping2 and hping3, Xmas scanning networks on targeted IP's.	K3
CO2	Make up the ideas in service enumeration tools like SuperScan and Softperfect.	K6
CO3	Apply knowledge on vulnerabilities scanning using Nessus tool and the system hacking tools like winrtgen .	K3
CO4	Determine the knowledge on Capture network packets using whireshark, Social Engineering Attack using Kali Linux	K5
CO5	Apply the idea on malware threats using HTTP RAT Torjan, TCP/IP Connections using currport tool.	K3
CO6	Infer the exposure on DOS attacks using Metasploit and Hping3	K2

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**
CO1												
CO2												
CO3												
CO4												
CO5												
CO6												

(Please fill the above with Levels of Correlation, viz., L, M, H)

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

Experiment- 1
Google Hacking Database

Experiment- 2
Scanning Networks to detect the Targeted IP
a) Nmap
b) hping2 and hping3
c) Xmas scanning

Experiment- 3
Service enumeration on Targeted IP
a) Nmap
b) SuperScan tool
c) Softperfect network scanner tool

Experiment- 4
Vulnerability scanning using Nessus vulnerability Scanning tool

Experiment- 5
System Hacking
a) System hacking for default passwords
b) Rainbow table using winrtgen tool

Experiment- 6
a) Create image steganography
b) Cleaning audit policies and logs on windows

Experiment- 7
Malware Threats
a) Create a HTTP RAT Trojan
b) Monitoring TCP/IP connection using currport tool

Experiment- 8
Capture network packets using whireshark

Experiment- 9
Social Engineering Attack using Kali Linux

Experiment- 10
Denial-of-Service
a) SYN Flooding Attack using Metasploit
b) SYN Flooding Attack using Hping3

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

Experiment- 11
Configure Honey pots on windows server 2016

Experiment- 12
Hacking Web Servers Foot printing using ID Server tool

Experiment- 13
SQL Injection using IBM Security AppScan Standard

Experiment- 14
Password Cracking:

a) Password cracking using pwdump7 and ophcrack
b) Password cracking using keyloggers

Experiment- 15
Study on all different types of Hacking Tools.

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M. Tech (CY) II Semester

Constitution of India

Code: R19MCY1258

Course Objectives:

- Understand the premises informing the twin themes of liberty and freedom from a civil rights perspective.
- To address the growth of Indian opinion regarding modern Indian intellectuals' constitutional role and entitlement to civil and economic rights as well as the emergence of nationhood in the early years of Indian nationalism.
- To address the role of socialism in India after the commencement of the Bolshevik Revolution in 1917 and its impact on the initial drafting of the Indian Constitution.

Course Outcomes: At the end of the course, student will be able to

	Course Outcomes	Knowledge Level (K)#
CO1	Discuss the growth of the demand for civil rights in India for the bulk of Indians before the arrival of Gandhi in Indian politics.	K6
CO2	Discuss the intellectual origins of the framework of argument that informed the conceptualization of social reforms leading to revolution in India.	K6
CO3	Discuss the circumstances surrounding the foundation of the Congress Socialist Party [CSP] under the leadership of Jawaharlal Nehru and the eventual failure of the proposal of direct elections through adult suffrage in the Indian Constitution.	K6
CO4	Discuss the passage of the Hindu Code Bill of 1956.	K6
CO5	Discuss the growth of the demand for civil rights in India for the bulk of Indians before the arrival of Gandhi in Indian politics.	K6

#Based on suggested Revised BTL

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												
CO4												
CO5												

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT–I: History of Making of the Indian Constitution: History, Drafting Committee, (Composition & Working)

UNIT–II: Philosophy of the Indian Constitution- Preamble, Salient, Features

UNIT–III: Contours of Constitutional Rights & Duties: Fundamental Rights, Right to Equality, Right to Freedom, Right against Exploitation, Right to Freedom of Religion, Cultural and Educational Rights, Right to Constitutional Remedies, Directive Principles of State Policy, Fundamental Duties.

UNIT–IV: Organs of Governance: Parliament, Composition, Qualifications and Disqualifications, Powers and Functions, **Executive-** President, Governor, Council of Ministers, Judiciary, Appointment and Transfer of Judges, Qualifications, Powers and Functions

UNIT–V: Local Administration: District's Administration head: Role and Importance, Municipalities: Introduction, Mayor and role of Elected Representative CEO of Municipal Corporation, Pachayati raj: Introduction, PRI: ZilaPachayat, Elected officials and their roles, CEO ZilaPachayat: Position and role, Block level: Organizational Hierarchy (Different departments), Village level: Role of Elected and Appointed officials, Importance of grass root democracy

UNIT–VI: Election Commission: Election Commission: Role and Functioning, Chief Election Commissioner and Election Commissioners, State Election Commission: Role and Functioning, Institute and Bodies for the welfare of SC/ST/OBC and women.

Text Books:

1. The Constitution of India, 1st Edition, (Bare Act), Government Publication, 1950
2. Framing of Indian Constitution, 1st Edition, Dr. S. N. Busi, Dr. B. R. Ambedkar 2015

Reference Books:

1. Indian Constitution Law, 7th Edition, M. P. Jain, Lexis Nexis, 2014

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M. Tech (CY) II Semester

Pedagogy Studies

Code: R19MCY1258

Course Objectives:

Students will be able to:

- Review existing evidence on the review topic to inform programme design and policy making undertaken by the DfID, other agencies and researchers.
- Identify critical evidence gaps to guide the development.

Course Outcomes: At the end of the course, student will be able to

	Course Outcomes	Knowledge Level (K)#
CO1	What pedagogical practices are being used by teachers in formal and informal classrooms in developing countries?	K1
CO2	What is the evidence on the effectiveness of these pedagogical practices, in what conditions, and with what population of learners?	K1
CO3	How can teacher education (curriculum and practicum) and the school curriculum and guidance materials best support effective pedagogy?	K1

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**
CO1												
CO2												
CO3												

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT–I: Introduction and Methodology: Aims and rationale, Policy background, Conceptual framework and terminology, Theories of learning, Curriculum, Teacher education, Conceptual framework, Research questions**,** Overview of methodology and Searching.

UNIT–II: Thematic overview: Pedagogical practices are being used by teachers in formal and informal classrooms in developing countries, Curriculum, Teacher education.

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

UNIT–III: Evidence on the effectiveness of pedagogical practices: Methodology for the in depth stage: quality assessment of included studies, How can teacher education (curriculum and practicum) and the school curriculum and guidance materials best support effective pedagogy, Theory of change, Strength and nature of the body of evidence for effective pedagogical practices, Pedagogic theory and pedagogical approaches, Teachers' attitudes and beliefs and Pedagogic strategies.

UNIT–IV: Professional development: Alignment with classroom practices and follow-up support, Peer support, Support from the head teacher and the community, Curriculum and assessment, Barriers to learning: limited resources and large class sizes

UNIT–V: Research gaps and future directions: Research design, Contexts, Pedagogy, Teacher education, Curriculum and assessment, Dissemination and research impact.

Text Books:

1. Classroom interaction in Kenyan primary schools, Ackers J, Hardman F, Compare, 31 (2): 245-261, 2001
2. Curricular reform in schools: The importance of evaluation, Agrawal M, Journal of Curriculum Studies, 36 (3): 361-379, 2004

Reference Books:

3. Teacher training in Ghana: does it count? Multi-site teacher education research project (MUSTER) country report 1, Akyeampong K, London: DFID, 2003

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M. Tech (CY) II Semester

Stress Management by Yoga

Code: R19MCY1258

Course Objectives:

- To achieve overall health of body and mind
- To overcome stress

Course Outcomes: At the end of the course, student will be able to

	Course Outcomes	Knowledge Level (K)#
CO1	Develop healthy mind in a healthy body thus improving social health also	K2
CO2	Improve efficiency	K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT–I: Definitions of Eight parts of yog. (Ashtanga)

UNIT–II: Yam and Niyam. Do`s and Don't's in life.

i) Ahinsa, satya, astheya, bramhacharya and aparigraha
ii) Shaucha, santosh, tapa, swadhyay, ishwarpranidhan

UNIT–III: Asan and Pranayam

i) Various yoga poses and their benefits for mind & body
ii) Regularization of breathing techniques and its effects-Types of pranayam

Text Books:

1. Yogic Asanas for Group Tarining-Part-I :Janardan Swami Yogabhyasi Mandal, Nagpur
2. Rajayoga or conquering the Internal Nature, Swami Vivekananda, AdvaitaAshrama Publication Department, Kolkata

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M. Tech (CY) II Semester

Personality Development through Life Enlightenment Skills

Code: R19MCY1258

Course Objectives:

- To learn to achieve the highest goal happily
- To become a person with stable mind, pleasing personality and determination
- To awaken wisdom in students

Course Outcomes: At the end of the course, student will be able to

	Course Outcomes	Knowledge Level (K)#
CO1	Study of Shrimad-Bhagwad-Geeta will help the student in developing his personality and achieve the highest goal in life	K2
CO2	The person who has studied Geeta will lead the nation and mankind to peace and prosperity	K3
CO3	Study of Neetishatakam will help in developing versatile personality of students.	K5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT–I: Neetisatakam-Holistic development of personality, Verses- 19,20,21,22 (wisdom), Verses- 29, 31, 32 (pride & heroism), Verses- 26,28,63,65 (virtue), Verses- 52, 53, 59 (don'ts), Verses- 71,73,75,78 (do's)

UNIT–II: Approach to day to day work and duties.
Shrimad Bhagwad Geeta: Chapter 2-Verses 41, 47, 48

UNIT–III: Chapter 3-Verses 13, 21, 27, 35, Chapter 6-Verses 5, 13, 17, 23,35, Chapter 18- Verses 45, 46, 48

UNIT–IV: Statements of basic knowledge.

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

Shrimad Bhagwad Geeta: Chapter2-Verses 56, 62, 68
Chapter 12 -Verses 13, 14, 15, 16, 17, 18

UNIT–V: Personality of Role model. Shrimad Bhagwad Geeta: Chapter2-Verses 17, Chapter 3-Verses 36, 37, 42,
Chapter 4-Verses 18, 38, 39
Chapter18 – Verses 37, 38, 63

Text Books:

1. Srimad Bhagavad Gita, Swami Swarupananda Advaita Ashram (PublicationDepartment), Kolkata
2. Bhartrihari's Three Satakam (Niti-sringar-vairagya), P.Gopinath

Reference Books:

1. Rashtriya Sanskrit Sansthanam, New Delhi.

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M.Tech (CY) III Semester

Cyber Security Governance

Code: R19MCY2351

Course Objectives:

- Knowledge and understanding of the different theories on cyber-governance, the implications of cyberspace
- Understanding the internet for traditional notions such as sovereignty, power, war and conflict, terrorism and crime.
- Understanding the historical developments in cyber governance and how key events have led to the current state of affairs.

Course Outcomes: At the end of the course, student will be able to

	Course Outcomes	Knowledge Level (K)#
CO1	Explain the fundamental concepts and principles of the cyber Security Governance and theories of governance.	K2
CO2	Demonstrate the metrics of Cyber Security Governance.	K2
CO3	Explain the principal driving force for Cyber security governance is risk management, which involves mitigating risks and reducing or preventing potential impact on information resources.	K5
CO4	Model the enterprise needs metric against which to judge Cyber security policy to ensure that organizational objectives are achieved.	K3
CO5	Explore the Threat Intelligence Governance and Industrial Governance.	K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												
CO4												
CO5												

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT–I: Cyber security Governance-Principles of cyber security governance, Assessment of cyber security maturity. Theories of governance: introduction, Governance – definitions and typologies, Tools, methods and processes.

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

UNIT–II: Network Device metrics-Vulnerability management, Threat management, Endpoint management, Intrusion detection and prevention (IDPS), Security incident management, Security operations centre (SOC) and related concepts.

UNIT–III: Measurement of Governance-Metrics – concepts, Application security metrics, Network security metrics, Security incident metrics, Vulnerability metrics, Service level objectives / agreement (SLO / SLA), NIST metrics.

UNIT–IV: Security analytics Governance-Basics of security analytics, Threat intelligence and governance, Data driven security governance, Impact of cognitive security on security governance.

UNIT–V: Industry Governance-Industry specific security compliance, Cyber security governance India and Other countries, NIST mandates for compliance, Security reporting basics, CISO – role and organization structure.

Text Books:

1. IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data, Hayden, lance, McGraw-hill education group, 2010
2. Data-Driven Security: Analysis,1st Edition, Visualization and Dashboards, Jacobs, Jay, and Bob Rudis, John wiley & sons, 2014

Reference Books

1. Cyber Security, Critical Infrastructure, Framework for Improving Critical Infrastructure Cyber Security, Framework, 1st Edition 2014

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M.Tech (CY) III Semester

Principles of Secure Coding

Code: R19MCY2352

Course Objectives:

- Understanding of the various security attacks and knowledge to recognize and remove common coding errors that lead to vulnerabilities.
- Knowledge of outline of the techniques for developing a secure application.
- Recognize opportunities to apply secure coding principles.

Course Outcomes: At the end of the course, student will be able to

	Course Outcomes	**Knowledge Level (K)#**
CO1	Outline the secure systems and various security attacks	K2
CO2	Demonstrate the development of process of software leads to secure coding practices	K2
CO3	Apply Secure programs and various risk in the software's	K3
CO4	Classify various errors that lead to vulnerabilities	K4
CO5	Design Real time software and vulnerabilities	K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**
CO1												
CO2												
CO3												
CO4												
CO5												

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT–I: Introduction- Need for secure systems, Proactive security development process, Security principles to live by and threat modelling.

UNIT–II: Secure Coding in C- Character strings- String manipulation errors, String Vulnerabilities and exploits Mitigation strategies for strings, Pointers, Mitigation strategies in pointer based vulnerabilities Buffer Overflow based vulnerabilities

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

UNIT–III: Secure Coding in C++ and Java- Dynamic memory management, Common errors in dynamic memory management, Memory managers, Double –free vulnerabilities, Integer security, Mitigation strategies

UNIT–IV: Database and Web Specific Input Issues- Quoting the Input, Use of stored procedures, Building SQL statements securely, XSS related attacks and remedies

UNIT–V: Software Security Engineering- Requirements engineering for secure software: Misuse and abuse cases, SQUARE process model Software security practices and knowledge for architecture and design

Text Book:

1. Writing Secure Code, 2nd Edition, Michael Howard, David LeBlanc, Microsoft Press, 2003

Reference Books:

1. Secure Coding in C and C++, Robert C. Seacord, 2nd edition, Pearson Education, 2013
2. Software Security Engineering: A guide for Project Managers, 1st ed, Julia H. Allen, Sean J. Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead, Addison-Wesley Professional, 2008

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M.Tech (CY) III Semester

Information System Audit

Code: R19MCY2353

Course Objectives:

- Understanding and knowledge of Security Auditing, and introduce the Threats and defense in the systems.
- Acquiring the knowledge on Evidence collection and evaluation techniques.

Course Outcomes: At the end of the course, student will be able to

	Course Outcomes	Knowledge Level (K)#
CO1	Illustrate the fundamental concepts of information security and systems auditing	K2
CO2	Analyze the latest trend of computer security threats and defense	K4
CO3	Identify security weaknesses in information systems, and rectify them with appropriate security mechanisms	K3
CO4	Explain the security controls in the aspects of physical, logical and operational security control and case studies	K5
CO5	Evaluate the security of information systems	K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												
CO4												
CO5												

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT–I: Overview of Information System Auditing- Effect of Computers on Internal Controls, Effects of Computers on Auditing, Foundations of information Systems Auditing, Conducting an Information Systems Audit.

UNIT–II: The management Control Framework-I- Introduction, Evaluating the planning Function, Leading Function, Controlling Function, Systems Development Management Controls, Approaches to Auditing Systems Development, Normative Models of the Systems Development Process, Evaluating the Major phases in the Systems Development Process, Programming Management Controls, Data Resource Management Controls.

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

UNIT–III: The Management Control Framework-II- Security Management Controls, Operations management Controls Quality assurance Management Controls, Case Studies.

UNIT–IV: Evidence Collection- Audit Software, Code Review, Test Data, and Code Comparison, Concurrent Auditing techniques, Interviews, Questionnaires, and Control Flowcharts. Performance Management tools- Case Studies.

UNIT–V: Evidence Evaluation- Evaluating Asset Safeguarding and Data Integrity, Evaluating System, Effectiveness, Evaluating System Efficiency, Information Systems Audit and Management: Managing the Information Systems Audit Function.

Reference Books:

1. Information Systems Control and Audit, 1st Edition, Ron Weber, Pearson Education, 2013
2. Information System Audit and Assurance, D P Dube, TMH, New Delhi, 2008

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M.Tech (CY) III Semester

Python Programming

Code: R19MCY2352

Course Objectives:

- Knowledge and understanding of the different concepts of Python.
- Using the GUI Programming and Testing in real-time applications.
- Using package Python modules for reusability.

Course Outcomes: At the end of the course, student will be able to

	Course Outcomes	Knowledge Level (K)#
CO1	Demonstrate and comprehend the basics of python programming.	K2
CO2	Demonstrate the principles of structured programming and be able to describe, design, implement, and test structured programs using currently accepted methodology.	K3
CO3	Explain the use of the built-in data structures list, sets, tuples and dictionary.	K5
CO4	Make use of functions and its applications.	K3
CO5	Identify real-world applications using oops, files and exception handling provided by python.	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												
CO4												
CO5												

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT–I: Introduction- History of Python, Python Language, Features of Python, Applications of Python, Using the REPL (Shell), Running Python Scripts, Variables, Assignment, Keywords, Input-Output, Indentation.

UNIT–II: Types, Operators and Expressions-Types - Integers, Strings, Booleans; Operators- Arithmetic Operators, Comparison (Relational) Operators, Assignment Operators, Logical Operators, Bitwise Operators, Membership Operators, Identity

Operators, Expressions and order of evaluations, Control Flow- if, if-elif-else, for, while, break, continue, pass.

UNIT–III: Data Structures-Lists - Operations, Slicing, Methods; Tuples, Sets, Dictionaries, Sequences, Comprehensions.

UNIT–IV: Functions- Defining Functions, Calling Functions, Passing Arguments, Keyword Arguments, Default Arguments, Variable-length arguments, Anonymous Functions, Fruitful Functions(Function Returning Values), Scope of the Variables in a Function - Global and Local Variables, Modules: Creating modules, import statement, from.. import statement, name spacing, Python packages, Introduction to PIP, Installing Packages via PIP, Using Python Packages Error and Exceptions: Difference between an error and Exception, Handling Exception, try except block, Raising Exceptions, User Defined Exceptions.

UNIT–V: Object Oriented Programming OOP in Python-Classes, 'self variable', Methods, Constructor Method, Inheritance, Overriding Methods, Datahiding, Brief Tour of the Standard Library - Operating System Interface - String Pattern Matching, Mathematics, Internet Access, Dates and Times, Data Compression, Multithreading, GUI Programming, Turtle Graphics, Testing: Why testing is required ?, Basic concepts of testing, Unit testing in Python, Writing Test cases, Running Tests.

Text Books

1. Python Programming: A Modern Approach, 1st Edition ,Vamsi Kurama, Pearson, 2018
2. Learning Python,1st Edition, Mark Lutz, Orielly, 2013

Reference Books:

1. Think Python, Allen Downey, Green Tea Press, 2012
2. Core Python Programming, W. Chun, Pearson, 2013
3. Introduction to Python,1st Edition, Kenneth A. Lambert, Cengage, 2013

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M.Tech (CY) I Semester

Principles of Cyber Security

Code: R19MCY2352

Course Objectives:

- To learn threats and risks within context of the cyber security architecture.
- Student should learn and Identify security tools and hardening techniques.
- To learn types of incidents including categories, responses and timelines for response.

Course Outcomes: At the end of the course, student will be able to

Course Outcomes		Knowledge Level (K)#
CO1	Apply cyber security architecture principles.	K3
CO2	Demonstrate the risk management processes and practices.	K2
CO3	Appraise cyber security incidents to apply appropriate response	K5
CO4	Distinguish system and application security threats and vulnerabilities.	K4
CO5	Identify security tools and hardening techniques	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												
CO4												
CO5												

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT–I: Introduction to Cyber security- Cyber security objectives**,** Cyber security roles**,** Differences between Information Security & Cyber security. Cyber security Principles- Confidentiality, integrity, &availability Authentication & non repudiation.

UNIT–II: Information Security (IS) within Lifecycle Management-Lifecycle management landscape, Security architecture processes, Security architecture tools,

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

Intermediate lifecycle management concepts, Risks & Vulnerabilities-Basics of risk management**,** Operational threat environments**,** Classes of attacks.

UNIT–III: Incident Response- Incident categories**,** Incident response Incident recovery. Operational security protection: Digital and data assets, ports and protocols, Protection technologies, Identity and access Management, configuration management.

UNIT–IV: Threat Detection and Evaluation (DE): Monitoring- Vulnerability Management, Security Logs and Alerts, Monitoring Tools and Appliances**.** Analysis-Network traffic Analysis, packet capture and analysis

UNIT–V: Introduction to backdoor System and security-Introduction to metasploit, Backdoor, demilitarized zone(DMZ),Digital Signature, Brief study on Harding of operating system.

Text Books:

1. NASSCOM: Security Analyst Student Hand Book, Dec 2015
2. Information Security Management Principles, Updated Edition, David Alexander, Amanda Finch, David Sutton, BCS publishers, June 2013

Reference Books:

1. Cyber Security Fundamentals-Cyber Security, Network Security and Data Governance Security, 2nd Edition, ISACA Publishers

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M.Tech (CY) III Semester

Internet of Things

Code: R19MCY2352

Course Objectives:

- Identify problems that are amenable to solution by AI methods, and which AI methods may be suited to solving a given problem.
- Formalize a given problem in the language/framework of different AI methods.
- Implement basic AI algorithms.
- Design and carry out an empirical evaluation of different algorithms on problem formalization, and state the conclusions that the evaluation supports.

Course Outcomes: At the end of the course, student will be able to

Course Outcomes		Knowledge Level (K)#
CO1	Explain the definition and usage of the term 'the internet of things' in different contexts	K5
CO2	Discover the various network protocols used in IoT	K3
CO3	Be familiar with the key wireless technologies used in IoT systems, such as Wi-Fi, 6LoWPAN, Bluetooth and ZigBee	K4
CO4	Illustrate the role data analytics in a typical IoT system	K2
CO5	Design a simple IoT system made up of sensors, wireless network connection, data analytics and display/actuators, and write the necessary control software	K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												
CO4												
CO5												

(Please fill the above with Levels of Correlation, viz., L, M, H)

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

UNIT I: The Internet of Things- An Overview of Internet of Things, Internet of Things Technology, behind IoTs Sources of the IoTs, M2M Communication, Examples of IoTs, Design Principles For Connected Devices

UNIT II: Business Models for Business Processes in the Internet of Things, IoT/M2M systems LAYERS AND designs standardizations ,Modified OSI Stack for the IoT/M2M Systems, ETSI M2M domains and High-level capabilities, Communication Technologies, Data Enrichment and Consolidation and Device Management Gateway Ease of designing and affordability

UNIT III: Design Principles for the Web Connectivity for connected-Devices, Web Communication protocols for Connected Devices, Message Communication protocols for Connected Devices, Web Connectivity for connected-Devices.

UNIT IV: Data Acquiring, Organizing and Analytics in IoT/M2M, Applications/ Services/ Business Processes, IOT/M2M Data Acquiring and Storage, Business Models for Business Processes in the Internet Of Things, Organizing Data, Transactions, Business Processes, Integration and Enterprise Systems.

UNIT V: Data Collection, Storage and Computing Using a Cloud Platform for IoT/M2M Applications /Services, Data Collection, Storage and Computing Using cloud platform Everything as a service and Cloud Service Models, IOT cloud-based services using the Xively (Pachube/COSM), Nimbits and other platforms Sensor, Participatory Sensing, Actuator, Radio Frequency Identification, and Wireless, Sensor Network Technology, Sensors Technology, Sensing the World.

Text Books:

1. Internet of Things: Architecture, Design Principles and Applications, 1st Edition, Rajkamal, McGraw Hill Higher Education, 2017.
2. Internet of Things, 1st ed, A.Bahgya and V.Madisetti, Univesity Press, 2015.
3. Internet of Things from Hype to Reality: The road to Digitization, 1st Edition, Ammar Rayes Samersalam, 2016.

Reference Books:

1. Designing the Internet of Things, 1st ed, Adrian McEwen and Hakim Cassimally, Wiley, 2013.
2. Getting Started with the Internet of Things, 1st ed, CunoPfister , Oreilly, 2011.
3. Internet of Things and Data Analytics Handbook, 1st ed, HWAIYU GENG, Wiley publications, 2017.

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

M.Tech (CY) III Semester

Artificial Intelligence and Machine Learning

Code: R19MCY2352

Course Objectives:

- To learn the basic concepts and techniques of AI and machine learning
- To explore the various mechanism of Knowledge and Reasoning used for building expert system.
- To become familiar with supervised and unsupervised learning models
- To design and develop AI and machine learning solution using modern tools.

Course Outcomes: At the end of the course, student will be able to

Course Outcomes		Knowledge Level (K)#
CO1	Explain the fundamentals of AI and machine learning	K2
CO2	Identify an appropriate AI problem solving method and knowledge representation technique	K3
CO3	Identify appropriate machine learning models for problem solving	K3
CO4	Design and develop the AI applications in real world scenario	K6
CO5	Compare the relationship between AI, ML, and Deep Learning	K2

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1												
CO2												
CO3												
CO4												
CO5												

(Please fill the above with Levels of Correlation, viz., L, M, H)

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

UNIT– I: Introduction to AI- Definition, Problem, State space representation. Intelligent Systems: Categorization of Intelligent System, Components of AI Program, Foundations of AI, Applications of AI, Current trends in AI, Intelligent Agents: Anatomy, structure, Types.

UNIT– II: Problem solving-Solving problem by Searching: Problem Solving Agent, Formulating Problems. Uninformed Search Methods: Breadth First Search (BFS), Depth First Search (DFS), Depth Limited Search, Depth First Iterative Deepening (DFID), Informed Search Methods- Greedy best first Search, A* Search, Memory bounded heuristic Search. Local Search Algorithms and Optimization Problems- Hill climbing search Simulated annealing and local beam search.

UNIT – III: Knowledge and Reasoning-Knowledge based Agents, The Wumpus World, and Propositional logic**. First Order Logic**- Syntax and Semantic, Inference in FOL, Forward chaining, backward Chaining, Knowledge Engineering in First-Order Logic, Unification and Resolution.

UNIT – IV: Concepts of Machine learning -Supervised, unsupervised, semi-supervised, Rote learning, Reinforcement learning, Issues, steps and applications, Designing a learning System. Case study- hand written digit recognition, stock price prediction. Learning Models- Decision tree learning. Probabilistic Models, Deterministic Models, Hidden Markov Model, Reinforcement Learning-Model based learning, Temporal Difference Learning, Generalization, Partially Observable States.

UNIT – V: Artificial Neural Network: Introduction, neural network representation, Problems for neural network learning, perception, multilayer network & Back propagation Algorithm**.** Deep learning- Definition, relationship between AI, ML, and Deep Learning, Trends in Deep Learning.

Text Books:

1. Artificial Intelligence and Machine Learning, 1st Edition, Vinod Chandra S.S., Anand Hareendran S, 2014
2. Artificial Intelligence: A Modern Approach, 2nd Edition, Pearson Education, Stuart J. Russell, Peter Norvig, 2002
3. Machine Learning, 1st ed, McGraw-Hill Education, Tom M. Mitchell, 1997
4. Introduction to machine learning, 2nd edition, The MIT Press, Ethem Alpaydin 2010

Department of Computer Science & Engineering
University College of Engineering, JNT University Kakinada

Reference Books:

1. PROLOG Programming for Artificial Intelligence", 3rd Edition, Pearson Education, Ivan Bratko, 2002
2. Artificial Intelligence, Third Edition, McGraw Hill Education, Elaine Rich and Kevin Knight, 2017
3. Data Mining Concepts and Techniques, Morgann Kaufmann Publishers, Han Kamber, 2011
4. Machine learning with R, 2nd Edition, Brett Lantz, 2015
5. Genetic Algorithms: Search, Optimization and Machine Learning, 1st ed, Davis E. Goldberg, Addison Wesley, N.Y., 1989