JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

Vision and Mission of the University

VISION

The University is primarily promoting quality of education in the areas of Science, Technology, Engineering and Mathematics (STEM) as four academic pillars of education, to excel in teaching, learning, research, consultancy and placements through innovative practices with global perspective.

MISSION

1. Design an Industry relevant curriculum from time to time with a Global perspective
2. Promoting quality education by embracing ICT delivery mechanism with continuous pedagogy through e-learning mechanism
3. Spread across for industry collaborations with a focus to pre-training and placements for technology transfer to society
4. Establishing centers of excellence to promote research and innovations in multidisciplinary areas to bring in patent culture and consultancy practices
5. International Collaborations for student outreach
6. Facilitating international students to study in JNTUK to infuse cross culture learning practices.

Vision and Mission of the Institute

Vision and Mission of the Department

Programme Education Objectives (PEOs) of the M.Tech - CYBER SECURITY

PEO1: To equip students with a comprehensive understanding of mathematical foundations, machine learning techniques, and optimization strategies, enabling them to apply this knowledge effectively in solving complex real world problems.

PEO2: To foster a research-oriented mindset and encourage innovation in the field of machine learning. Graduates should be capable of conducting independent research, contributing to advancements in machine learning techniques, and developing novel solutions to emerging challenges.

PEO3: To promote ethical practices, intellectual property rights awareness, and holistic development. Graduates should possess strong communication skills, an understanding of societal implications, and a commitment to values such as sustainability, social responsibility, and continuous learning.

Mapping of Mission statements to PEOs:

Mission Statement	PEO1	PEO2	PEO3
MS1	✓	✓	✓
MS2	✓	✓	✓
MS3	✓	✓	✓
MS4	✓	✓	✓
MS5		✓	✓
MS6		✓	✓

Programme Outcomes (POs)

PO1: An ability to independently carry out research /investigation and development work to solve practical problems

PO2: An ability to write and present a substantial technical report/document

PO3: Students should be able to demonstrate a degree of mastery over the area as per these Specializations of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program

PO4: Understanding of theoretical foundations of computing and, modelling and design of Artificial Intelligence (AI) systems.

PO5: Able to assess the significance of a complex AI problem and analyse its characteristics.

PO6: Ability to explore contemporary research issues and gaps, and to propose original ideas and solutions in AI

Note: Program may add up to three additional Pos Mapping of Programme Outcomes to PEOs:

Programme Outcomes (POs)	PEO1	PEO2	PEO3
PO1	2	3	1
PO2	1	2	3
PO3	3	2	1
PO4	3	2	1
PO5	3	2	1
PO6	2	3	1

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

M.Tech

CYBER SECURITY

Programme Course Structure & Syllabus

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

R25 MTech - Cyber Security Structure

I Semester

S.No	Course Title	L	T	P	C
1	**Program Core-1** Mathematical Foundations for Cyber Security	3	1	0	4
2	**Program Core-2** Incident Response and Threat Intelligence	3	1	0	4
3	**Program Core-3** Applied Cryptography	3	1	0	4
4	**Program Elective-1** • Firewall and VPN Security • Malware Analysis and Detection • Internet of Things Security	3	0	0	3
5	**Program Elective-2** • Design of Secure Operating Systems • Web Application security • Hardware Security	3	0	0	3
6	**Laboratory-1** Incident Response and Threat Intelligence Lab	0	1	2	2
7	**Laboartory-2** Applied Cryptography Lab	0	1	2	2
8	**Seminar-1**	0	0	2	1
	Total Credits	15	5	6	23

List of Professional Elective Courses in I Semester (Electives – I & II)

S.No.	Course Title
1	Firewall and VPN Security
2	Malware Analysis and Detection
3	Internet of Things Security
4	Design of Secure Operating Systems
5	Web Application security
6	Hardware Security

@ Minimum 2/3 themes per elective

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

II Semester

S.No	Course Title	L	T	P	C
1	**Program Core-4** Digital Forensics	3	1	0	4
2	**Program Core-5** Secure System Development	3	1	0	4
3	**Program Core-6** Penetration testing & Vulnerability Analysis	3	1	0	4
4	**Program Elective-3** • Blockchain Application Security and Investigation • Post Quantum Cryptography • Artificial Intelligence & Machine Learning in Cyber security	3	0	0	3
5	**Program Elective-4** • Database Security • Cloud Security • Malware Analysis & Reverse Engineering	3	0	0	3
6	**Laboratory-3** Digital Forensics Lab	0	1	2	2
7	**Laboartory-4** Penetration testing & Vulnerability Analysis Lab	0	1	2	2
8	**Seminar-2**	0	0	2	1
	Total Credits	15	5	6	23

During the summer break, students need to pursue Summer Internship/ Industrial Training, which will be evaluated in the III Sem.

List of Professional Elective Courses in II Semester (Electives III & IV)

S.No.	Course Title
1	Blockchain Application Security and Investigation
2	Post Quantum Cryptography
3	Artificial Intelligence & Machine Learning in Cyber security
4	Database Security
5	Cloud Security
6	Malware Analysis & Reverse Engineering

@ Minimum 2/3 themes per elective

III Semester

S.No	Course Code	Course Title	L	T	P	C
1		Research Methodology and IPR / Swayam 12-week MOOC course – RM&IPR	3	0	0	3
2		Summer Internship/ Industrial Training (8-10 weeks)*	-	-	-	3
3		Comprehensive Viva#	-	-	-	2
		Dissertation Part – A$			20	10
Total Credits			3		20	18

** Student attended during summer/year break, and assessment will be done in the third semester.*

 # Comprehensive viva can be conducted for courses completed up to the second semester.

$ Dissertation – Part A, internal assessment

IV Semester

S.No	Course Code	Courses	L	T	P	C
1		Dissertation Part – B%	-	-	32	16
Total Credits						16

% External Assessment

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

I Semester	MATHEMATICAL FOUNDATIONS FOR CYBER SECURITY	L	T	P	C
		3	1	0	4

Course Objectives:

1. To provide a strong foundation in number theory, algebraic structures, probability theory, coding theory, and pseudorandom number generation,
2. enabling students to apply mathematical concepts and computational techniques for problem-solving, cryptography, and secure communication systems.

Course Outcomes: At the end of the course, student will be able to (Four to Six)

		Knowledge Level (K)#
CO1	Apply number theory concepts and theorems, including congruences and the Chinese remainder theorem, to solve computational problems.	K3
CO2	Understand algebraic structures such as groups, rings, fields, and lattices for cryptographic applications.	K2
CO3	Apply probability theory, stochastic processes, and Markov chains in problem-solving and modeling	K3
CO4	Design and evaluate coding schemes for error detection and correction using linear and advanced codes	K5
CO5	Implement and assess pseudorandom number generators for secure cryptographic operations.	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1			H	H	M	
CO2			H	H	M	
CO3			H	M	M	
CO4			H	H	H	
CO5			H	M	H	

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

UNIT	CONTENTS	Contact Hours
UNIT – 1	NUMBER THEORY: Introduction - Divisibility - Greatest common divisor - Prime numbers – Fundamental theorem of arithmetic - Mersenne primes - Fermat numbers - Euclidean algorithm - Fermat's theorem -Euler totient function - Euler's theorem. Congruences: Definition - Basic properties of congruences -Residue classes - Chinese remainder theorem.	12
UNIT – 2	ALGEBRAIC STRUCTURES: Groups – Cyclic groups, Cosets, Modulo groups - Primitive roots – Discrete logarithms. Rings – Sub rings, ideals and quotient rings, Integral domains. Fields – Finite fields – GF (pn),GF(2n) - Classification - Structure of finite fields. Lattice, Lattice as Algebraic system, sub lattices, some special lattices.	12
UNIT – 3	PROBABILITY THEORY: Introduction – Concepts of Probability - Conditional Probability - Baye's Theorem - Random Variables – discrete and continuous- central Limit Theorem-Stochastic Process-Markov Chain.	12
UNIT – 4	CODING THEORY: Introduction - Basic concepts: codes, minimum distance, equivalence of codes, Linear codes - Linear codes - Generator matrices and parity-check matrices - Syndrome decoding –Hamming codes - Hadamard Code - Goppa codes.	12
UNIT – 5	PSEUDORANDOM NUMBER GENERATION: Introduction and examples - Indistinguishability of Probability Distributions - Next Bit Predictors - The Blum-Blum-Shub Generator – Security of the BBS Generator.	12
	Total	60

REFERENCES:

1. Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, 'An introduction to the theory of numbers', John Wiley and Sons 2004.
2. Douglas Stinson, 'Cryptography – Theory and Practice', CRC Press, 2006.
3. Sheldon M Ross, "Introduction to Probability Models", Academic Press, 2003.
4. C.L. Liu, 'Elements of Discrete mathematics', McGraw Hill, 2008.
5. Fraleigh J. B., 'A first course in abstract algebra', Narosa, 1990.
6. Joseph A. Gallian, ''Contemporary Abstract Algebra', Narosa, 1998.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

I Semester	INCIDENT RESPONSE AND THREAT INTELLIGENCE	L	T	P	C
		3	1	0	4

Course Objectives:

1. Provide a thorough understanding of incident response and threat intelligence processes.
2. Equip students with practical skills for managing and handling cybersecurity incidents.
3. Develop expertise in leveraging threat intelligence for risk management and vulnerability assessment.
4. Learn the incident handling process, incident prioritization, and the impact of virtualization on response techniques.
5. Explore the role of Security Operations Centers (SOCs), logs, and log management in incident response.
6. Apply threat intelligence for vulnerability management and risk assessment using frameworks like MITRE ATT&CK and the Cyber Kill Chain.
7. Apply tools and techniques for effective threat hunting and incident response.

Course Outcomes: At the end of the course, student will be able to (Four to Six)

		Knowledge Level (K)#
CO1	Apply key concepts of information security and incident response to identify and categorize different computer security incidents based on real-world scenarios.	K3
CO2	Apply Security Operations Center (SOC) strategies and log management techniques to detect, analyze, and report security incidents effectively.	K3
CO3	Analyse the threat intelligence lifecycle and the differences between tactical, operational, and strategic intelligence in incident handling	K4
CO4	Analyse and utilize threat intelligence models and frameworks to assess and manage risks in vulnerability management.	K4
CO5	Create PowerShell scripts to automate threat-hunting processes, including identifying malicious processes and conducting remote incident response tasks.	K5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1			H	H	M	
CO2		M		H	H	
CO3			H	H	M	
CO4			H	H	H	
CO5				H	H	

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

UNIT	CONTENTS	Contact Hours
UNIT – 1	**Introduction to Incident Response** Cyber Incident Statistics, Computer Security Incidents, Information Warfare o Key concepts of Information Security, Types of Computer Security Incidents Examples of Computer Security Incidents , How to identify an incident? Need for Incident Response ,Goals and Purpose of Incident Response ,Signs of an Incident- Precursors &Indicators , Incident Categories.	12
UNIT – 2	Incident Management and Handling Incident Handling Process, Incident Prioritization, Impact of Virtualization on Incident Response & Handling ,Estimating Cost of an Incident, Incident Reporting & Reporting Standards, Incident Reporting Organizations ,Vulnerability Resources , Introduction to Security Operations Center (SOC) 24 , Working on SOC o Introduction to Logs, Types and Sources of Logs , Need for Log Management Challenges of Log Management ,Incident Response Tools and Techniques.	12
UNIT – 3	Threat Intelligence in Incident Handling, What is Threat Intelligence, Data versus Intelligence, Need for Threat Intelligence Threat Intelligence Process Model, Threat Intelligence Life Cycle o Levels of Threat Intelligence, Threat Intelligence Challenges	12
UNIT – 4	Threat Intelligence for Vulnerability and Risk Management, What is Risk Management , Assess Risk based on Exploitability, Exploitability versus Exploitation ,Sources of Intelligence , Cross-Referencing Intelligence , The Fair Play Model , The Lockheed Martin Cyber Killing Chain , The Diamond Model, The MITRE ATT&CK Framework.	12
UNIT – 5	Threat Hunting Using PowerShell Introduction to Threat Hunting Threat Hunting Tools & Techniques , Introduction to PowerShell , Environment SetuWorking with PowerShell Scripts, cmdlets, files & folders, dates and times, File I/O , Advanced Cmdlets , PowerShell Scripting, special variables, operators, looping, conditions, array, hash tables, regex, PowerShell Advanced Functions, , Objects in Windows PowerShell; Error Handling Concepts, terminating & nonterminating errors , Using PowerShell to Formulate the Hunt – List & Identify the Processes, use of CIM, , PowerShell remoting capabilities: remoting concepts, invoking remote commands, processing outputs.	12
	Total	60

Textbooks:

1. Leighton Johnson, “Computer Incident Response and Forensics Team Management: Conducting Successful Incident Response”, First Edition, Syngres, 2013
2. Jithin Abey Alex, “Incident Handling and Response: A Holistic Approach for an Efficient Security Incident Management”, First Edition,2020 References: 1. Murdoch, D. W, “Blue Team Handbook: incident response”, First Edition, CreateSpace Independent Publishing, 2016 2. Steve Anson, “Applied Incident Response” First Edition, Wiley, 2020
3. Arun E Thomas, “Security Operations Center- SIEM Use Cases and Cyber Threat Intelligence”, First Edition, Independent Publisher, 2018
4. Luttgens, Jason T., Matthew Pepe, and Kevin Mandia, “Incident response & computer forensics”, McGraw-Hill Education Group, 2014
5. Chris Hawley, Rob Schnepp, and Ron Vidal, “Incident Management for Operations”, First edition, O'Reilly Media, Inc., 2017
6. Gerard Johansen, “Digital Forensics and Incident Response: Incident Response Techniques and Procedures to Respond to Respond to Modern Cyber Threats, Second Edition, Packt Publishers, 2020

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

I Semester	APPLIED CRYPTOGRAPHY	L	T	P	C
		3	1	0	4

Course Objectives:

1.To equip students with the knowledge and skills.

*2.*to design, analyze, and implement cryptographic techniques for ensuring confidentiality, integrity, authentication, and secure communication in real-world applications.

Course Outcomes: At the end of the course, student will be able to (Four to Six)

		Knowledge Level (K)#
CO1	Explain basic and advanced cryptographic protocols and their applications.	K2
CO2	Apply key management techniques and cipher modes for secure communication.	K3
CO3	Use symmetric and asymmetric algorithms for data encryption and security.	K3
CO4	Implement hash functions and message authentication codes for integrity and authentication.	K5
CO5	Apply public-key algorithms, digital signatures, and secure communication standards.	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1			H	H	M	
CO2			H	H	M	
CO3			H	H	M	
CO4			H	H	M	
CO5			H	H	M	
CO6						

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

UNIT	CONTENTS	Contact Hours
UNIT – 1	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.	12
UNIT – 2	Information Theory, Complexity Theory, Number Theory, Factoring,	12

	Prime Number Generation, Discrete Logarithms in a Finite Field, Data Encryption Standard (DES), IDEA, CAST, Blowfish, RC5, Double Encryption, Triple Encryption.	
UNIT – 3	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.	12
UNIT – 4	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.	12
UNIT – 5	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).	12
	Total	60

Text Books:

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

Reference Books:

1. Modern Cryptography Theory and Practicel, Wenbo Mao, Pearson Education, 2004
2. Cryptography and network security, Behrouz A. Forouzan, McGraw-Hill, Inc., 2008

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

I Semester	FIREWALL AND VPN SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

1. To provide students with the knowledge and skills.
2. to design, configure, and manage firewalls and VPN solutions for protecting network infrastructure, ensuring secure remote access, and mitigating security threats.

Course Outcomes: At the end of the course, student will be able to (Four to Six)

		Knowledge Level (K)#
CO1	Explain the fundamentals, goals, and policies of network security along with common threats and attacker techniques.	K2
CO2	Describe network topologies, security components, and firewall implementation for secure network design.	K2
CO3	Apply packet filtering, proxy servers, and VPN technologies to secure network communication.	K3
CO4	Analyze and manage IDS/IPS architectures, interoperability models, and security approaches.	K4
CO5	Configure and evaluate IDS tools like Snort to detect, prevent, and respond to network intrusions.	K5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1			M	H	M	
CO2			M	H	M	
CO3				H	H	
CO4			M	H	H	
CO5				H	H	

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

UNIT	CONTENTS	Contact Hours
UNIT – 1	**Fundamentals of Network Security:** Introduction, network Security, Seven Domains of a Typical IT Infrastructure, Goals of Network Security, Measure the Success of Network Security, Network Security Policies Important, Internal and External Network Issues, Common Network Security Components Used to Mitigate Threats, TCP/IP Basics. **Network Security Threats:** Hackers and Their Motivation, Favorite Targets of Hackers,	12

	Threats from Internal Personnel and External Entities, The Hacking Process, Common IT Infrastructure Threats Malicious Code (Malware), Advanced Persistent Threat, Session Hijacking, Spoofing, and Man-in-the-Middle Attacks, Covert Channels, Hacker Tools, Social Engineering.	
UNIT – 2	Common Network Topologies and Infrastructures, Network Design Considerations, Firewall Fundamentals, Firewall Implementation, Firewall Deployment Considerations, Configuring Firewalls.	12
UNIT – 3	**Packet Filtering:** Introduction, Understanding Packets and Packet Filtering, Packet-Filtering Methods, Setting Specific Packet Filter Rules, Hands-On Projects. **Working with Proxy Servers and Application-Level Firewalls:** Proxy Servers, Benefits of Proxy Servers, Configuring Proxy Servers, Choosing a Proxy Server, Proxy Server-Based Firewalls Compared.	12
UNIT – 4	VPN Fundamentals, VPN Management, VPN Technologies, VPN Implementation, Firewall Security Management, Best Practices for Network Security Management Emerging Technology and Regulatory Considerations.	12
UNIT – 5	**IDS infrastructure**: IDS Architecture, IDS/IPS Management and Architecture Issues with regard to deploying IDS/IPS systems, end point approach to security, system approach to security, IDS Interoperability models: CIDF (Common Intrusion Detection Framework), IDMEF (Intrusion Detection Message Exchange Format), IODEF (Incident Object Description Exchange Format), CVE (Common Vulnerabilities and Exposures), OVAL (Open Vulnerability and Assessment Language). **IDS tools:** Snort and Bro IDS tools, NIDS Evasion, Insertion, and Checksums to confuse NID systems, Snort Fundamentals and Configuration, Snort GUIs & Sensor Management, Snort Performance, Active Response & Tagging, Snort Rules, Stimulus Response, hosts response to both normal and abnormal traffic, Advanced Snort Concepts as rule ordering and reduction of false negatives and positives. Evaluation and tuning of IDS, Cross over Rate (CER) of IDS.	12
	Total	60

Text Books:

1. Network Security, Firewall and VPNs, Third Edition. J. Michael Stewart, Denise Kinsey, 2020.
2. Guide to Firewalls and VPNs Michael E. Whitman, Herbert J. Mattord, Andrew Green, 2012.
3. Network Intrusion Detection, Stephen Narthcutt, 2002.
4. CCNP Security: Intrusion Prevention and Intrusion Detection Systems, David Burns, Odunayo Adesina, Keith Barker, Cisco Press, 2012.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

I Semester	MALWARE ANALYSIS AND DETECTION	L	T	P	C
		3	0	0	3

Course Objectives:

1. To enable students to understand, analyze, and detect malicious software by applying static and dynamic analysis techniques
2. Reverse engineering, and security tools for effective threat mitigation

Course Outcomes: At the end of the course, student will be able to (Four to Six)

		Knowledge Level (K)#
CO1	Understand the malware and life cycle and Analysis setup	K2
CO2	Apply the distribution mechanism in malware analysis	K3
CO3	Discuss the static and dynamic analysis of malwares	K2
CO4	Analyze the malware detection methods and reverse engineering approaches	K4
CO5	Learn Malware Reverse Engineering & Detection Engineering	K2

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1			M	H	M	
CO2				H	M	
CO3			M	H	H	
CO4				H	H	
CO5				H	H	
CO6						

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

UNIT	CONTENTS	Contact Hours
UNIT – 1	**Introduction:** Types of Malware, Malware attack Life Cycle, Malware Business model, Malware Analysis setup, Operating Systems Files and File formats.	12
UNIT – 2	**System Fundamentals:** Virtual memory and Portable Executable Files, Windows Internals – Win32 API, Registry, Directories, Processes and services	12
UNIT – 3	**Malware Components**: Malware Components , Distribution mechanisms, Malware Packers, Persistence mechanism, Network Communication, Detecting Network Communication, Code Injection, Process Hollowing, API Hooking, Stealth techniques and Rootkits	12

UNIT – 4	**Malware Analysis and Classification:** Static Analysis, Dynamic Analysis , Memory Forensics with Volatility, Malware Payload dissection and Classification.	12
UNIT – 5	**Malware Reverse Engineering:** Debuggers and disassembly, Debugging for unpacking malware and code injections, Armoring Techniques Detection Engineering : Device Analysis, Anti Virus Engines, IDS/IPS and Snort /Suricata rule writing, Malware Sandbox Internals, DBI for Malware analysis	12
	Total	60

Text Book

1. Ahijit Mohanta, Anoop Saldanha, Malware Analysis and Detection Engineering: A Comprehensive Appraoch to Detect and Analyze Modern Malware, Apress Berkeley, CA, 2020.
2. Michael Sikorski and Andrew Honig, “Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software”, No Starch Press, 2012.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

I Semester	INTERNET OF THINGS SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

1. To provide learners with a comprehensive understanding of IoT security principles
2. To enabling them to identify vulnerabilities, design robust security architectures.
3. To implement effective protection mechanisms to safeguard IoT devices, networks, and applications against potential threats.

Course Outcomes: At the end of the course, student will be able to (Four to Six)

		Knowledge Level (K)#
CO1	Explain IoT architecture, security requirements, benefits, and privacy concerns.	K2
CO2	Identify IoT vulnerabilities, attack models, and common IoT-specific cyberattacks.	K4,K2
CO3	Apply security measures to IoT networking functions, communication links, and back-end systems.	K3
CO4	Implement hardware and software security mechanisms for IoT devices and applications.	K5
CO5	Analyze real-world IoT attack case studies and recommend preventive security strategies.	K4

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1			M	M		M
CO2			M	H	M	
CO3				H	H	
CO4				H	H	
CO5	M			H	H	M

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

UNIT	CONTENTS	**Contact Hours**
UNIT – 1	**IoT-Security Overview:** IoT, Architecture of IoTs, IoT Security Requirements (Privacy preservation, Device security, authentication, confidentiality and integrity), Benefits & Applications of IoT, IoT Attack Surface, Industrial Standards and Evolution. Device security, Gateway security, IoT Privacy Concerns, Privacy by Design, Conducting a PrivacyImpact Assessment, Case Study: The Connected Barbie.	12
UNIT – 2	**IoT- Security & Vulnerability Issues:** IoT Vulnerabilities -Secret-Key,	12

	Authentication/Authorization for Smart Devices, Constrained, System Resources, Device Heterogeneity, Fixed Firmware. Attack Models - Layer-wise Attack model, Attacks to Sensors in IoTs, Attacks to RFIDs in IoTs, Attacks to Network Functions in IoTs, Attacks to Back-end Systems, Security in Front-end Sensors and Equipment. IoT Attacks - Side-channel Attacks, Spoofing Attack, Sniffing Attack, Rogue Devices Attack, Man-in-Middle Attack, DDoS Attack, Sensor base Attack.	
UNIT – 3	**Securing internet of things environments:** Networking Function Security - IoT Networking Protocols, Layering Architecture, Secure IoT Lower Layers, Secure IoT Higher Layers, Secure Communication Links in IoTs, Back-end Security- Secure Resource Management, Secure IoT Databases.	12
UNIT – 4	IoT Hardware -Test Device Range, Latency and Capacity, Manufacturability Test, Secure from Physical Attacks. IoT Software -Trusted IoT Application Platforms, Secure Firmware Updating, Network Enforced Policy, Secure Analytics Visibility and Control.	12
UNIT – 5	IoT attacks- case study: MIRAI Botnet Attack, Iran's Nuclear Facility Stuxnet Attack, Tesla Crypto jacking Attack, The Spam-haus attack, Traffic Light Hacks, DDoS spoofing attack against American health insurance provider.	12
	Total	60

Text Book

1. Fei HU, Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations, CRC Press, 2016.
2. Ollie Whitehouse, Security of Things: An Implementers' Guide to Cyber-Security for Internet of Things Devices and Beyond NCC Group, 2014.
3. Russell, Brian and Drew Van Duren, Practical Internet of Things Security , Packet Publishing, 2016.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

I Semester	DESIGN OF SECURE OPERATING SYSTEMS	L	T	P	C
		3	0	0	3

Course Aims and Objectives:

1. Develop a comprehensive understanding of operating system security architectures and their implications for overall system security.
2. Master the techniques for identifying, analyzing, and mitigating common and advanced security vulnerabilities in operating systems.
3. Design and implement robust security mechanisms for critical OS components, including access control systems, memory management, and process isolation.
4. Evaluate and critique existing operating system security measures, and propose improvements based on current best practices and emerging threats.
5. Gain practical experience in secure OS development through hands-on projects, fostering skills in secure coding, testing, and debugging of OS-level security features.

Course Outcomes: At the end of the course, student will be able to (Four to Six)

		Knowledge Level (K)#
CO1	Explain the fundamentals of secure operating systems, security goals, trust models, and threat models.	K2
CO2	Describe access control mechanisms, protection systems, and secure OS assessment criteria.	K2
CO3	Analyze the Multics operating system architecture, security models, and vulnerability analysis.	K4
CO4	Apply information flow security and integrity models such as Bell-LaPadula and Biba for system protection.	K3
CO5	Evaluate secure capability systems and secure virtual machine systems for trusted computing environments.	K5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1			M	M		M
CO2			M	H	M	
CO3			M	H	M	
CO4			M	H	M	
CO5	M		M	H	M	

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

UNIT	CONTENTS	Contact Hours
UNIT – 1	Introduction : Secure Operating Systems , Security Goals , Trust	12

	Model , Threat Model. Access Control Fundamentals o Protection System Lampon's Access Matrix Mandatory Protection System Reference Monitor Secure Operating System Definition Assessment Criteria.	
UNIT – 2	Multics : Multics ,Multics History ,The Multics System , Multics Fundamentals , Multics Security Fundamentals ,Multics Protection System Models ,Multics Protection System , Multics Reference Monitor, Multics Security- Multics Vulnerability Analysis. ,Security in Ordinary Operating Systems-System Histories	12
UNIT – 3	Verifiable Security Goals, Information Flow , Information Flow Secrecy Models , Denning's Lattice Model ,Bell-LaPadula Model ,Information Flow Integrity Models , Biba Integrity Model , Low-Water Mark Integrity , Clark-Wilson Integrity , The Challenge of Trusted Processes , Covert Channels , Channel Types-Noninterference.	12
UNIT – 4	Secure Capability Systems :Secure Capability Systems , Capability System Fundamentals , Capability Security-Challenges in Secure Capability Systems , Capabilities and the ^-Property , Capabilities and Confinement ,Capabilities and Policy Changes-Building Secure Capability Systems , Enforcing the ^-Property , Enforcing Confinement-Revoking Capabilities	12
UNIT – 5	Secure Virtual Machine Systems : Secure Virtual Machine Systems Separation Kernels o,VAX VMM Security Kernel ,VAX VMM Design ,VAX VMM Evaluation , VAX VMM Result , Security in Other Virtual Machine Systems.	12
	Total	60

Textbooks:

1. Operating System Security, Trent Jaeger, Morgan & Claypool Publishers, 2008.
2. Operating system internal and design principles: William Stallings.
3. The Design of the Unix Operating System, Maurice J Bach, PHI.

References:

1. Stallings (2006), Operating Systems, Internals and Design Principles, 5th edition, Pearson Education, India.
2. Andrew S. Tanenbaum (2007), Modern Operating Systems, 2nd edition, Prentice Hall of India.
3. Deitel & Deitel (2008), Operating systems, 3rd edition, Pearson Education, India.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

I Semester	WEB APPLICATION SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

1. To provide learners with an in-depth understanding of web application security principles
2. enabling them to identify vulnerabilities, assess risks, and implement secure coding practices
3. defense mechanisms to protect web applications against emerging threats.

Course Outcomes: At the end of the course, student will be able to (Four to Six)

		Knowledge Level (K)#
CO1	Understand the concepts of web application and and security principles	K2
CO2	Know Access control methods, Session Management Fundamentals	K2
CO3	Apply the web application security controls	K3
CO4	Analyze the systematic vulnerability detection	K4
CO5	Apply the file security and database security principles	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1			M	M		
CO2			M	M		
CO3				H	M	
CO4				H	H	
CO5				H	M	

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

UNIT	CONTENTS	Contact Hours
UNIT – 1	**Introduction:** Introduction to Web Application Security, OWASP list, Security Fundamentals: Input Validation, Attack Surface Reduction, Classifying and Prioritizing Threats. **Web Application Security Principles:** Authentication-Fundamentals, Two-factor and threefactor Authentication, Web Application Authentication, Securing password-based Authentication.	12
UNIT – 2	**Authorization:** Access control methods, Session Management	12

	Fundamentals. Database Security Principles: SQL Injection, Setting Database Permissions, Stored Procedure Security, Insecure Direct Object References.	
UNIT – 3	**File Security Principles:** Keeping Your Secure Code Secret, Security Through Obscurity, Forceful Browsing, Directory Traversal **Secure Development Methodologies:** Holistic Approach, Industry Standard Secure Development Methodologies and Maturity Models. DevSec Ops.	12
UNIT – 4	Web Application Reconnaissance, Structure of a Modern Web Application: REST APIs, SPA Frameworks, Finding Sub domains, API Analysis, Identifying third party dependencies and weak points in Application Architecture, web Application Firewall.	12
UNIT – 5	Vulnerability Discovery and Management, Defending Against XSS Attacks, CSRF Attacks, Defending Against XXE, Defending Against Injection and DoS, Securing Third-Party Dependencies.	12
	Total	60

Text Book

1. Bryan Sullivan, Vincent Liu, “Web Application Security”, McGraw Hill, 2012.
2. Dafydd Stuttard Marcus Pinto, “The Web Application Hacker’s Handbook”, Wiley Publishing Inc., 2008.

I Semester	HARDWARE SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

1. To impart a comprehensive understanding of hardware security principles
2. To enabling learners to identify potential threats, analyze vulnerabilities in hardware systems.
3. design robust protection mechanisms to ensure the confidentiality, integrity, and reliability of hardware-based components and architectures.

Course Outcomes: At the end of the course, student will be able to (Four to Six)

		Knowledge Level (K)#
CO1	Explain the fundamentals of hardware security, threats, vulnerabilities, and countermeasures.	K2
CO2	Describe SoC, PCB, and embedded system security concepts, design flows, and testing methods.	K2
CO3	Analyze hardware attacks such as Trojans, side-channel, test-oriented, and physical attacks.	K4
CO4	Apply hardware security primitives, obfuscation techniques, and authentication methods for secure hardware design.	K3
CO5	Evaluate emerging trends, system-level security, and trust assessment techniques in hardware security.	K5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1			M	M		
CO2			M	M	M	
CO3			M	H	H	
CO4				H	H	
CO5	M			M	M	M
CO6						

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

UNIT	CONTENTS	Contact Hours
UNIT – 1	**Introduction to Hardware Security:** Overview of a Computing System, Layers of a Computing System, What Is Hardware Security, Hardware Security vs. Hardware Trust, Attacks, Vulnerabilities, and Counter measures, Conflict Between Security and Test/Debug, Evolution of Hardware Security	12

	A Quick Overview of Electronic Hardware: Introduction, Nanoscale Technologies, Digital Logic, Circuit Theory, ASICs and FPGAs, Printed Circuit Board, Embedded Systems , Hardware-Firmware-Software Interaction. System on Chip (SoC) Design and Test: Introduction, The IP-Based SoC Life-Cycle, SoCDesign Flow, SoC Verification Flow, SoC Test Flow, Design-for-Debug, Structured DFT Techniques Overview, At-Speed Delay Test. Printed Circuit Board (PCB): Design and Test: Introduction, Evolution of PCB and Components, PCB Life Cycle, PCB Assembly Process, PCB Design Verification	
UNIT – 2	**HARDWARE ATTACKS:** ANALYSIS, EXAMPLES, AND THREAT MODELS Hardware Trojans: Introduction, SoC Design Flow, Hardware Trojans, Hardware Trojans in FPGA Designs, Hardware Trojans Taxonomy, Trust Benchmarks Counter measures Against Hardware Trojans. **Electronics Supply Chain:** Introduction, Modern Electronic Supply Chain, Electronic Components Supply Chain Issues, Security Concerns, Trust Issues, Potential Countermeasures. Hardware IP Piracy and Reverse Engineering: Introduction, Hardware Intellectual Property (IP), Security Issues in IP-Based SoC Design, Security Issues in FPGA.	12
UNIT – 3	**Side-Channel Attacks:** Introduction Background on Side-Channel Attacks Power Analysis Attacks, Electromagnetic (EM) Side-Channel Attacks Fault Injection Attacks, Timing Attacks **Test-Oriented Attacks:** Introduction, Scan-Based Attacks JTAG-Based Attacks, Hands-on Experiment: JTAG Attack. **Physical Attacks and Countermeasures:** Introduction Reverse Engineering, Probing Attack, Invasive Fault Injection Attack. **Attacks on PCB:** Security Challenges and Vulnerabilities: Introduction, PCB Security Challenges: Attacks on PCB, Attack Models. Secure Element.	12
UNIT – 4	**Counter Measures against Hardware Attacks** **Hardware Security Primitives:** Introduction, Preliminaries, Physical Unclonable Function	12

	True Random Number Generator, Design for Anti-Counterfeit Existing Challenges and Attacks, Primitive Designs With Emerging Nano devices. Security and Trust Assessment, and Design for Security: Introduction, Security Assets and Attack Models Pre-silicon Security and Trust Assessment for SoCs, Post-silicon Security and Trust Assessment for ICs, Design for Security **Hardware Obfuscation**: Introduction Overview of Obfuscation Techniques, Hardware Obfuscation Methods, Emerging Obfuscation Approaches, Use of Obfuscation Against Trojan Attacks.	
UNIT – 5	**PCB Authentication and Integrity Validation** : PCB Authentication , Sources of PCB Signature, Signature Procurement and Authentication Methods, Signature Assessment Metric, Emerging Solutions, PCB Integrity Validation EMERGING TRENDS IN HARDWARE ATTACKS AND PROTECTIONS System Level Attacks & Countermeasures, Introduction, Background on SoC Design, SoC Security Requirements, Security Policy Enforcement, Secure SoC Design Process, Threat Modeling, Hands-on Experiment: SoC Security Policy. STQC Specifications.	12
	Total	60

Text Book

1. Hardware Security: A Hands-On Learning Approach, Mark Tehranipoor and Swarup Bhunia, 2018.
2. Hardware Security: Design, Threats, and Safeguards, Debdeep Mukhopaday, Rajat Subhra Chakaraborthy, 2014

I Semester	INCIDENT RESPONSE AND THREAT INTELLIGENCE LAB	L	T	P	C
		0	1	2	2

Course Objectives:

1. Understand the incident response lifecycle and the roles/responsibilities involved.
2. Practice triaging and mitigating real-world attack scenarios using industry-standard tools.
3. Learn to preserve and analyze logs, system images, and memory dumps.
4. Explore Indicators of Compromise (IoCs), Tactics, Techniques and Procedures (TTPs), and threat actor profiling

Course Outcomes: At the end of the course, student will be able to (Four to Six)

		Knowledge Level (K)#
CO1	Identify and classify cybersecurity incidents based on severity and type using systematic investigation techniques.	K3
CO2	Demonstrate hands-on proficiency in digital forensic tools and evidence acquisition procedures.	K4
CO3	Implement appropriate incident response strategies using standard operating procedures (SOPs) and tools.	K3
CO4	Apply threat intelligence techniques to identify Indicators of Compromise (IoCs) and track threat actors.	K4
CO5	Analyze case studies and generate detailed technical reports on incident handling and threat analysis.	K5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	L		M	M		
CO2			M	M	M	L
CO3	L	L	M	H	H	
CO4				H	H	
CO5	M	H	L	M	M	M
CO6						

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

LIST OF EXPERIMENTS	CONTENTS
EXP–1	Implement penetration testing and phases of penetration testing
EXP–2	Make use of different types of tools available in kali and parrot O.S
EXP–3	Practice different SQL injection attacks
EXP–4	Implement and use GHDBC and Microsoft Vulnerabilities (Common

	CVE)
EXP–5	Implement Exploit insecure file handling, upload web shells, deface using upload file mechanism
EXP–6	Perform XSS attacks on client side application
EXP–7	Implement a case on actions on-behalf users by CSRF, Test websites for Click jacking
EXP–8	Implement port scanning by using NMAP and other tools to find the open ports
EXP–9	Text for wireshark and tcp dumps to analyze various types of packets
EXP–10	Implement Password attacks with methods like Dictionary Files - Key-space Brute Force - Pwdump and Fgdump - Windows Credential Editor (WCE- Exercises - Password Profiling - Password Mutating
EXP–11	Implement metasploit frameworks
EXP–12	Practice ARP spoofing and buffer overflow exploitation with ETERCAP AND SHELL'S
	Total

List of open Source software/learning Websites:

1. https://www.hackthebox.eu/
2. https://practicalpentestlabs.com/
3. https://pentesterlab.com

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

I Semester	APPLIED CRYPTOGRAPHY LAB	L	T	P	C
		0	1	2	2

Course Objectives:

1. To defend the security attacks on information systems with secure algorithms.
2. To learn advanced concepts of cryptography
3. To study concepts of security

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Analyze cryptographic concepts such as encryption, decryption, key management, cryptographic algorithms, and protocols	K4
CO2	Analyze the security of cryptographic systems, including understanding potential vulnerabilities and threats	K4
CO3	Apply cryptography in various real-world scenarios, including data protection, secure communication, and authentication.	K3
CO4	Implementing cryptographic algorithms and protocols using programming languages or cryptographic libraries.	K5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1			M	H	M	
CO2			M	H	M	
CO3				H	H	
CO4				H	H	

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

UNIT	CONTENTS
Experiment-1	Write a Java program to perform addition and multiplication in a finite field with a given prime modulus. Test your program with different inputs.
Experiment-2	Write a Java program to find the greatest common divisor (GCD) of two numbers using Euclid's algorithm. Test your program with various pairs of numbers.
Experiment-3	Implement a Java program that performs arithmetic operations (addition, subtraction, multiplication, and division) within a finite field GF(p), where "p" is a prime number provided by the user. The program should

	prompt the user to input two elements of the finite field and then perform the specified operations. Ensure that division by zero is handled appropriately, and the results are displayed modulo the prime modulus.
Experiment-4	Write a Java program to determine whether a given number is a probable prime using Fermat's Little Theorem. Allow the user to input the number and the desired number of iterations for the test.
Experiment-5	Implement a Java program to solve a system of linear congruence's using the Chinese Remainder Theorem.
Experiment-6	Write a Java program to find the modular inverse of a number using the Extended Euclidean Algorithm.
Experiment-7	Write a Java program to calculate Euler's Totient Function (phi) for a given positive integer.
Experiment-8	Develop a Java program to generate RSA public and private key pairs.
Experiment-9	Develop a program to generate Elliptic Curve Cryptography (ECC) key pairs. Support different elliptic curves and key lengths
Experiment-10	Write a Java program to create and verify digital signatures using the RSA.
Experiment-11	Write a program to perform digital signatures using the Elliptic Curve Digital Signature Algorithm
Experiment-12	Implement a MAC algorithm that uses a cryptographic hash function (e.g., SHA256) to generate the code. Ensure that the MAC provides both message integrity and authenticity.
Experiment-13	Create a program that verifies the integrity of a message using a MAC. Demonstrate how an attacker attempting to modify the message would be detected.
Experiment-14	Write a java program to demonstrate a basic timing attack on RSA decryption.
Experiment-15	Design and implement a java program that combines digital signatures with biometric authentication for enhanced security.
Experiment-16	Write a program that verifies the digital signature of a given message using a public key.

Text Books:

1. Bruce Schneier, Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C (cloth)
2. Atul Kahate,"Cryptography and Network Security", Third Edition, Mc. Graw Hill, 2014.
3. Johannes A. Buchmann, "Introduction to Cryptography", Springer-Verlag, 2001.
4. Bruce Schiener, "Applied Cryptography", Second Edition, Wiley, 2015.

Reference Books:

1. Oded Goldreich ,"Foundations of Cryptography", Cambridge University Press, 2001.

2. Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, “A Handbook of Applied Cryptography”, CRC Press, 1996.
3. Wembo Mao, “Modern Cryptography: Theory and Practice”, Pearson Education, 2003.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

II Semester	DIGITAL FORENSICS	L	T	P	C
		3	1	0	4

Course Objectives:

1. To provide learners with a comprehensive understanding of digital forensics principles
2. To equipping them with the skills to collect, preserve, analyze, and present digital evidence in accordance with legal and ethical standards for investigating cyber incidents.

Course Outcomes: At the end of the course, student will be able to (Four to Six)

		Knowledge Level (K)#
CO1	Apply memory analysis tools and file system analysis techniques to detect anti forensics	K3
CO2	Understand privacy issues and able to use live/Online forensic tools.	K2
CO3	Analyze windows registry, Linux server configurations and Apache server to identify incidents	K4
CO4	Analyze SQL databases and reconstruct activities by using SQL server toolkits	K4
CO5	Use Network Traffic analysis tools and collect evidences from network devices.	K2

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1				H	H	
CO2				M	M	
CO3				H	H	
CO4				H	H	
CO5				H	H	

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

UNIT	CONTENTS	Contact Hours
UNIT – 1	**File Systems:** FAT/NTFS file systems, Parsing FAT/NTFS file systems, Pre fetch and Super fetch, Shortcuts and Jumplists **Adversary and Malware hunting**: Malware detection, Malware analysis **Memory Forensics:** Memory acquisition, Memory analysis, memory analysis tools, Advanced Recycle bin, Server Logs, Google forensics. **Anti-Forensics Detection**: detection methodologies, Volume shadow copy, ESE databases, Advanced Registry, Thumbnail cache	12
UNIT – 2	**Computer Crime and legal issues:** Privacy issues, Intellectual	12

	property **Incident Response:** Threat and Adversary Intelligence, Financial crime analysis **Live/Online Forenics:** Live Digital Forensics Investigation. Tools: BitTorrent, Sleuthkit toolset, Windows Forensics. Tool chest Moot court: Moot court Case	
UNIT – 3	**Networking overview:** Windows Networks, Users and Groups, Introduction to Network Investigations **Windows and Linux servers:** Server roles, Server analysis, Windows Registry, Event logs Linux Forensics: Linux File systems, Linux server configurations, Linux artifacts, Apache server forensics, LAMP forensics, SMB and Linux file shares.	12
UNIT – 4	**IIS and Microsoft Exchange server:** IIS server, Mail server, Windows rootkits, Compromised server analysis. **SQL server and Data bases:** Microsoft SQL server, SQL server permission and encryption, SQL server Forensics Acquisition and analysis: SQL server forensics and traditional windows forensics, SQL server artifacts, Resident and non-resident artifact‟s Collecting SQL data bases, Creating an analysis database, Importing evidence, Activity Reconstruction, Data recovery, SQL server rootkits.	12
UNIT – 5	**Network Traffic Analysis:** Network addressing, DNS poisoning, ARP table analysis, DHCP analysis, Wire shark analysis. **Network Device Forensics:** management of switches and routers, Diagramming physical networks, Securing and isolating physical devices, Collecting Volatile/Non-volatile evidences from the routers, Volatile/Non-volatile.	12
	Total	60

Text Book:

1. H. Carvey, “Windows Forensics Analysis DVD Toolkit”, Syngress publishers 2009.
2. S. Anson, S. Bunting, R. Johnson, S. Perason, “Mastering Windows Network Forensics and Investigations”, Sybex publishers K. Fowler, SQL Server Forensic Analysis, Addison Wesley 2012.
3. K. Mandia, M. Pepe , J. Luttgens, “Incident Response & Computer Forensics”, Third Edition 2014.

4. M.H. Ligh, A. Case, J. Levy, A. waters, “The art of memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory”, Wiley 2014.
5. S. Davidoff, J. Ham, “Network Forensics: Tracking Hackers through Cyberspace”, Prentice Hall 2012.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

II Semester	SECURE SYSTEM DEVELOPMENT	L	T	P	C
		3	1	0	4

Course Objectives:

1. To provide learners with a thorough understanding of secure software and system development principles.
2. enabling them to design, implement, and maintain systems that incorporate security controls throughout the development lifecycle to protect against vulnerabilities and threats.

Course Outcomes: At the end of the course, student will be able to (Four to Six)

		Knowledge Level (K)#
CO1	Analyze software security vulnerabilities and apply best-practice practical techniques to prevent	K4
CO2	Apply wide-ranging technical and conceptual security skills to the software development lifecycle	K3
CO3	Demonstrate awareness of the complexity of contemporary software vulnerabilities and the techniques to discover and mitigate them.	K3
CO4	Demonstrate a systematic approach to problem solving and security planning.	K3
CO5	Understand Understanding Roles and Responsibilities of aTeam	K2

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1				H	H	
CO2				H	H	
CO3			M	H	M	
CO4				M	M	
CO5				M		M

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

UNIT	CONTENTS	**Contact Hours**
UNIT – 1	**Introduction:** Intersection of Security and Reliability , Understanding adversaries. Designing Systems: Case Study Safe Proxies, Design Tradeoffs, Design for Least Privilege.	12
UNIT – 2	Design for Understandability, Design for Changing Landscape,	12

	Design for Resilience, Design for recovery, Mitigating Denial-of-service Attacks.	
UNIT – 3	**Implementing Systems:** Designing, Implementing and Maintaining a publicly Trusted CA, Writing Code and Testing Code	12
UNIT – 4	Deploying Code and Investigating Systems. Maintaining Systems: Disaster Planning, Crisis Management , Recovery and Aftermath.	12
UNIT – 5	**Organization and Culture:** Case study: Chrome Security Team, Understanding Roles and Responsibilities , Building a Culture of Security and Reliability.	12
	Total	60

Text Book:

1. Ana Oprea, Betsy Beyer, Paul Blankinship Heather Adkins, Piotr Lewandowski, Adam Stubblefield, “Building Secure and Reliable Systems: Best Practices for Designing, Implementing, and Maintaining Systems”, O′Reilly; Edition 2020.
2. Julia H Allen, Sean J Barnum, Robert J Ellison, Gary McGraw, Nancy R Mead,
3. “Software Security Engineering: A Guide for Project Managers”, Addison Wesley, 2008.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

II Semester	PENETRATION TESTING AND VULNERABILITY ANALYSIS	L	T	P	C
		3	1	0	4

Course Objectives:

1. The course is taught with the objectives of enabling the student to:
2. Learn the theoretical basis for cyber threats and penetration testing phases and vulnerabilities
3. Perform protocol analysis using packet captures and analysis data using a sniffer
4. Apply testing methodologies using tools such as Wireshark, Nmap, Snort, Metasploit and related applications and platforms.

Course Outcomes: At the end of the course, student will be able to (Four to Six)

		Knowledge Level (K)#
CO1	Explain penetration testing concepts, categories, phases, and reporting methods.	K2
CO2	Apply information gathering, target enumeration, and port scanning techniques using security tools.	K3
CO3	Perform vulnerability scanning and assessment using tools like NMAP, Nessus, and Shodan.	K3
CO4	Conduct network sniffing, exploitation, password attacks, and post-exploitation activities.	K5
CO5	Demonstrate exploitation techniques in Windows, wireless, web, and mobile environments.	K5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1		M		H	M	
CO2				H	H	
CO3				H	H	
CO4				H	H	
CO5				H	H	
CO6						

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

UNIT	CONTENTS	Contact Hours
UNIT – 1	Introduction - Terminologies - Categories of Penetration Testing - Phases of Penetration Test- Penetration Testing Reports - Information Gathering Techniques - Active, Passive and Sources of Information Gathering - Approaches and Tools - Traceroutes, Neotrace, Whatweb, Netcraft, Xcode Exploit Scanner and NSlookup. Target	12

	Enumeration and Port scanning techniques - Host discovery - Scanning for open ports and services, Port scanning.	
UNIT – 2	Vulnerability Scanner Function, pros and cons - Vulnerability Assessment with NMAP - Testing SCADA environment with NMAP – Nessus, Vulnerability Scanner - Safe check - Silent dependencies - Port Range Vulnerability Data Resources, Network Sniffing, Shodan	12
UNIT – 3	Network Sniffing, Remote Exploitation, Capturing traffic: Networking for Capturing Traffic, Using Wireshark, ARP Cache Poisoning, DNS Cache Poisoning, SSL Attacks, SSL Stripping, Exploitation	12
UNIT – 4	Password Attacks: Password Management, Online Password Attacks, Offline Password Attacks. Client Side Exploitation and Post Exploitation	12
UNIT – 5	Windows Exploit Development Basics, Wireless Hacking and Attacks, Web hacking ,Mobile Hacking	12
	Total	60

Suggested Reading:

1. Rafay Baloch “Ethical Hacking and Penetration Testing Guide”, CRC Press, 2015.
2. Georgia Weidman, “Penetration Testing: A Hands-On Introduction to Hacking”, 2014.
3. Wil Allsopp, “Advanced Penetration Testing, Wiley, 2017.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

II Semester	BLOCKCHAIN APPLICATION SECURITY AND INVESTIGATION	L	T	P	C
		3	0	0	3

Course Objectives:

1. There is a trend towards central systems to systems without intermediaries.
2. The aim of this course is to teach students how these systems work and to gain the necessary knowledge and skills to develop codes on sample systems.
3. Topics covered include many emerging and current topics such as p2p network fundamentals, block chain technology, consensus protocols, deterministic programming, autonomous codes and smart contracts.
4. Quorum platform is chosen for software development and testing in this course, however the block chain platform that is used in this course may be changed according to the technological advancements.

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Explain cryptography, cryptocurrency fundamentals, and blockchain architecture with associated challenges.	K2
CO2	Develop and deploy smart contracts using Ethereum, Quorum, and Solidity.	K3
CO3	Analyze blockchain security issues, vulnerabilities, and defense mechanisms.	K4
CO4	Apply blockchain for decentralized storage, identity management, and trust systems.	K3
CO5	Use data analysis and forensic techniques to investigate blockchain transactions and detect malicious activity.	K4

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1			M	M		M
CO2				H	H	
CO3				H	H	
CO4				H	H	
CO5				H	H	

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

UNIT	CONTENTS	Contact Hours
UNIT – 1	Cryptography & Crypto Currency Fundamentals, Decentralized Systems (Block chain and derivatives) Fundamentals and Challenges,	12

	Introduction to Enterprise Block chain Solutions. Ethereum & Quorum Basics, Introduction to Deterministic Programming (Solidity Truffle).	
UNIT – 2	Ethereum Mechanics & Solidity, Team Project Proposal Presentations, Security and Issues, Cryptographic Tokens & Token Economy.	12
UNIT – 3	Security Philosophy & Block chain usage in Cyber Security, Distributed consensus, distributed ledgers, P2P Networking Foundations, Gossip and decentralized, collaboration.	12
UNIT – 4	Emerging Decentralized solutions for the Data Science, Decentralized storage, content distribution, Decentralized identity, Trust and reputation. Anonymous Communication. Understanding the cybersecurity aspects of blockchain, including potential vulnerabilities, attacks, and defense strategies.	12
UNIT – 5	Using data analysis techniques to track transactions, identify patterns, and detect suspicious activity on the blockchain, Learning about specialized tools and techniques for investigating blockchain-related crimes, including tracing transactions and identifying malicious actors.	12
	Total	60

Text Books:

1. Karaarslan, E., Konacaklı, E. "Data Storage in the Decentralized World: Blockchain and Derivatives". Kitap Bölümü. "Who Run The World: DATA" Kitabı. Istanbul University Press, 2020
2. Karaarslan E, Konacaklı E. "Decentralized solutions for data collection and privacy in healthcare", In D. Gupta, S. Bhattacharya, U. Kose, and Bao Le Nguyen (Eds.) Artificial intelligence for data-driven medical diagnosis. De Gruyter. ISBN: 978-3110667813, 2021.
3. Karaarslan, E., Aydin, D, "An AI Based Decision Support and Resource Management System for COVID-19 Pandemic", "DS for COVID-19" kitabı, Elsevier, 2021.

Reference:

1. Karaarslan, E., Birim M., "Blokzincirde Güvenlive Güvenilir Uygulama Geliştirme Temelleri", Siber Güvenlikve Savunma: Blokzincirive Kriptoloji, Nobel Yayınevi, 2021.
2. Konacaklı E., Karaarslan, E., "Blokzincirinin Askeri Lojistik TakipSistemlerinde Kullanılması", Siber GüvenlikveSavunma: BlokzinciriveKriptoloji, Nobel Yayınevi, 2021.
3. Karaarslan E., "Use of Blockchain Technology in the Health Sector" (Turkish), "Advanced Technology Applications in Health" Book, Nobel Publishing House, 2019
4. Kravchenko P., Skriabin B., Kurbatov O., Dubinina O. (2020). Blockchain And Decentralized Systems. Volume 1-3.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

II Semester	POST QUANTUM CRYPTOGRAPHY	L	T	P	C
		3	0	0	3

Course Objectives:

1. To provide learners with an in-depth understanding of cryptographic techniques resistant to quantum computing attacks.
2. To enabling them to analyze post-quantum algorithms.
3. evaluate their security and performance, and implement suitable solutions for future-proof secure communication systems.

Course Outcomes: At the end of the course, student will be able to (Four to Six)

		Knowledge Level (K)#
CO1	Understand the concepts of quantum computing, speedups offered by quantum algorithms	K2
CO2	Analyze the attacks on cryptography using quantum computers	K4
CO3	Analyze the cryptographic protocols using quantum key distribution	K4
CO4	Understand Lattice-based Cryptography & Digital Signatures	K2
CO5	Know about Multivariate Public Key Cryptography &Isogeney based Cryptography	K1

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1			M	M		M
CO2			M	H	M	
CO3			M	H	M	
CO4			M	M		
CO5			M	M		

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

UNIT	CONTENTS	Contact Hours
UNIT – 1	Introduction to post-quantum cryptography- Introduction and challenges Quantum computing: Classical and quantum Computing, Computation model, The quantum Fourier transform, The hidden subgroup problem, Search algorithms	12
UNIT – 2	Hash-based Digital Signature Schemes: Hash based one-time	12

	signature schemes, Merkle"s tree authentication scheme, One-time key-pair generation using an PRNG, Authentication path computation, Tree chaining, Distributed signature generation, Security of the Merkle Signature Scheme	
UNIT – 3	Code-based cryptography: Introduction, Cryptosystems, The security of computing syndromes as one-way function, Codes and structures, Practical aspects	12
UNIT – 4	Lattice-based Cryptography: Introduction, Preliminaries, Finding Short Vectors in Random q-ary Lattices, Hash Functions, Public Key Encryption Schemes, Digital Signature Schemes, Other Cryptographic Primitives.	12
UNIT – 5	Multivariate Public Key Cryptography: Introduction, The Basics of Multivariate PKCs, Examples of Multivariate PKCs, Basic Constructions and Variations, Standard Attacks. Isogeney based Cryptography: Supersigular Isogeny based Key Exchange (SIKE), Digital Signature Algorithm based on Isogeny	12
	Total	60

Text Book

1. Daniel J. Bernstein · Johannes Buchmann Erik Dahmen, "Post-Quantum Cryptography", Springer Verilag, 2009.
2. NIST Post Quantum Standardization- Specification document of the post-quantum secure Algorithms https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

II Semester	ARTIFICIAL INTELLIGENCE & MACHINE LEARNING IN CYBER SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

1. To provide learners with a comprehensive understanding of AI and ML techniques in the context of cyber security.
2. To enabling them to design, develop, and apply intelligent models for threat detection, anomaly analysis, malware classification, and automated incident response.

Course Outcomes: At the end of the course, student will be able to (Four to Six)

		Knowledge Level (K)#
CO1	Explain the fundamentals of AI and its applications in cybersecurity threat detection and prevention.	K2
CO2	Apply machine learning algorithms for spam, phishing, and malicious URL detection.	K3
CO3	Use time series analysis and ensemble methods to predict and detect cyber attacks.	K2
CO4	Implement AI techniques for CAPTCHA solving, fraud detection, and network anomaly detection.	K3
CO5	Utilize AI-based tools and platforms for cybersecurity data analysis and threat investigation.	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1			M	M	M	
CO2				H	H	
CO3				H	H	
CO4				H	H	
CO5				H	H	
CO6						

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

UNIT	CONTENTS	Contact Hours
UNIT – 1	Introduction to AI for Cyber security Applying AI in cyber security, The evolution from expert systems to data mining and AI, The different forms of automated learning, The characteristics of algorithm training and optimization, Introducing AI in the context of cyber security	12
UNIT – 2	AI for Cyber security Arsenal Classification, Regression,	12

	Dimensionality reduction, Clustering, Speech recognition, Video anomaly detection, Natural language processing (NLP), Large-scale image processing, Social media analysis Detecting Cyber security Threats with AI, How to detect spam with Perceptrons, Image spam detection with Support Vector Machines (SVMs), Phishing detection with logistic regression and decision trees, Spam detection with Naive Bayes, Spam detection adopting NLP.	
UNIT – 3	Basics of Machine Learning in Cyber security, Delving into machine learning in the cyber security world, Different types of machine learning systems, Different data preparation techniques, Machine learning architecture, statistical models and machine learning models, Model tuning to ensure model performance and accuracy, Machine learning tools Time Series Analysis and Ensemble Modeling Time series and its different classes, Time series decomposition, Analysis of time series in cyber security, Prediction of DDoS attack, Ensemble learning methods and voting ensemble methods to detect cyber attacks.	12
UNIT – 4	Segregating Legitimate and Lousy URLs Understanding URLs and how they fit in the internet address scheme, Introducing malicious URLs, Looking at the different ways malicious URLs propagate, Using heuristics to detect malicious URLs, Using machine learning to detect malicious URLs Knocking Down CAPTCHAs Characteristics of CAPTCHAs, Using artificial intelligence to crack CAPTCHAs, Types of CAPTCHA, Solving CAPTCHAs with neural networks.	12
UNIT – 5	Fraud Prevention with Cloud AI Solutions How to leverage machine learning (ML) algorithms for fraud detection, How bagging and boosting techniques can improve an algorithm's effectiveness, How to analyze data with IBM Watson and Jupyter Notebook, Using Data Science to Catch Email Fraud and Spam and Efficient Network Anomaly Detection Using k-means Fraudulent emails and spoofs, Types of email fraud, Spam detection using the Naive Bayes algorithm, Featurization techniques that convert text-based emails into numeric values, Spam detection with logistic regression	12
	Total	60

Text Book:

1. Alessandro Parisi, Hands-On Artificial Intelligence for Cyber security: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies, Packt Publication, 2019.
2. Clarence Chio and David Freeman, Machine Learning and Security: Protecting Systems with Data and Algorithms O‟REILLY Publications, 2018.

3. McKinney, W Brij B. Gupta and Quan Z. Sheng, Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices (Cyber Ecosystem and Security), CRC Press Publication, 2019.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

II Semester	DATABASE SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

1. To provide learners with a comprehensive understanding of database security principles
2. To enabling them to design and implement mechanisms for protecting data confidentiality, integrity, and availability, while mitigating threats, vulnerabilities, and unauthorized access.

Course Outcomes: At the end of the course, student will be able to (Four to Six)

		Knowledge Level (K)#
CO1	Explain database security models, access control mechanisms, and encryption techniques.	K2
CO2	Apply privacy-preserving methods such as k-anonymity, differential privacy, and steganographic file systems.	K3
CO3	Analyze and detect insider threats and anomalous access patterns in relational databases.	K4
CO4	Implement privacy-preserving query execution and aggregation over encrypted databases.	K3
CO5	Evaluate differential privacy techniques and their applications in data analysis and machine learning.	K5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1			M	M	M	
CO2				H	M	
CO3				H	H	
CO4				H	H	
CO5			M	M		

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

UNIT	CONTENTS	Contact Hours
UNIT – 1	Introduction, Design Principles, Discretionary Access Control, Virtual Private Database, Mandatory Access Control, Oracle Label Security	12
UNIT – 2	Role-based Access , Database as a Service I – Query, Encrypted Domain Keyword Search, Database as a Service II – Encryption-based, Executing SQL over encrypted data in the database-service-provider model, Efficient Execution of Aggregation Queries over	12

	Encrypted Relational Databases. Database Encryption	
UNIT – 3	**Data Privacy:** Review , Achieving k-anonymity privacy protection using generalization and suppression. Differential Privacy. Privacy in Location Based Service, Review, Steganographic File Systems, Insider Threat: Detecting anomalous access patterns in relational databases. Design and Implementation of an Intrusion Response System for Relational Databases.	12
UNIT – 4	The Promise of Differential Privacy: Privacy-preserving data analysis, Basic Terms, The model of computation, Towards defining private data analysis, Formalizing differential privacy. **Basic Techniques and Composition Theorems:** Useful probabilistic tools, Randomized response, The laplace mechanism, The exponential mechanism, Composition theorems, The sparse vector technique. Releasing Linear Queries with Correlated Error: An offline algorithm: SmallDB, An online mechanism: private multiplicative weights. Generalizations: Mechanisms via _-nets, The iterative construction mechanism, Connections	12
UNIT – 5	**Boosting for Queries:** The boosting for queries algorithm, Base synopsis generators. When Worst-Case Sensitivity is Atypical: Subsample and aggregate, Propose-test-Release, Stability and privacy. Lower Bounds and Separation Results: Reconstruction attacks, Lower bounds for differential privacy. **Differential Privacy and Computational Complexity**: Polynomial time curators, Some hard to-Syntheticize distributions, Polynomial time adversaries. Differential Privacy and Mechanism Design: Differential privacy as a solution concept, Differential privacy as a tool in mechanism design, Mechanism design for privacy aware agents **Differential Privacy and Machine Learning:** The sample complexity of differentially private machine learning, Differentially private online learning, Empirical risk minimization.	12
	Total	60

Text Book:

1. Christopher Diaz, Database Security: Problems and Solutions, Mercury Learning and Information, 2022
2. Cynthia Dwork, Aaron Roth , The Algorithmic Foundations of Differential Privacy , Now Publishers, 2014

3. Elisa Bertino, Ravi S. Sandhu: Database Security-Concepts, Approaches, and Challenges. IEEE Trans. Dependable Sec. Computing, VOL. 2, NO. 1, JANUARY-MARCH 2005
4. L. Sweeney: k-anonymity: a model for protecting privacy. Int. Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5):557-570, 2002.
5. A. Kamra, E. Terzi, E. Bertino: Detecting anomalous access patterns in relational databases. VLDB J. 17(5): 1063-1077 (2008)

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

II Semester	CLOUD SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

The course is taught with the objectives of enabling the student to:

1. Learn the concepts of distributed systems, algorithms and protocols
2. Understand the security in the cloud-infrastructure and analyze various attacks on cloud computing
3. Learn various cloud services and key management problems in cloud storage

Course Outcomes: At the end of the course, student will be able to (Four to Six)

		Knowledge Level (K)#
CO1	Explain cloud computing architecture, service models, deployment models, and associated security challenges.	K2
CO2	Apply compliance, audit, portability, and interoperability practices for secure cloud adoption.	K3
CO3	Implement business continuity, disaster recovery, and risk management strategies in cloud environments.	K3
CO4	Apply encryption, key management, and identity and access management techniques for cloud security.	K3
CO5	Evaluate virtualization technologies and implement security measures for virtualized cloud infrastructures.	K5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1			M	M	M	
CO2				H	M	
CO3				H	M	
CO4				H	H	
CO5				H	H	
CO6						

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

UNIT	CONTENTS	Contact Hours
UNIT – 1	**Cloud Computing Architectural Framework:** Cloud Benefits, Business scenarios, Cloud Computing Evolution, cloud vocabulary, Essential Characteristics of Cloud Computing, Cloud deployment models, Cloud Service Models, Multi- Tenancy, Approaches to create a barrier between the Tenants, cloud computing vendors, Cloud Computing threats, Cloud Reference Model, The Cloud Cube Model, Security for Cloud Computing, How Security Gets Integrated	12

UNIT – 2	**Compliance and Audit:** Cloud customer responsibilities, Compliance and Audit Security Recommendations. Portability and Interoperability: Changing providers reasons, Changing providers expectations, Recommendations all cloud solutions, IaaS Cloud Solutions, PaaS Cloud Solutions, SaaS Cloud Solutions.	12
UNIT – 3	Traditional Security, Business Continuity, Disaster Recovery, Risk of insider abuse, Security baseline, Customers actions, Contract, Documentation, Recovery Time Objectives (RTOs), Customers responsibility, Vendor Security Process (VSP).	12
UNIT – 4	Data Center Operations, Security challenge, Implement Five Principal Characteristics of Cloud Computing, Data center Security Recommendations. Encryption and Key Management: Encryption for Confidentiality and Integrity, Encrypting data at rest, Key Management Lifecycle, Cloud Encryption Standards, Recommendations	12
UNIT – 5	Identity and Access Management in the cloud, Identity and Access Management functions, Identity and Access Management (IAM) Model, Identity Federation, Identity Provisioning Recommendations, Authentication for SaaS and Paas customers, Authentication for IaaS customers, Introducing Identity Services, Enterprise Architecture with IDaaS, IDaaS Security Recommendations. **Virtualization:** Hardware Virtualization, Software Virtualization, Memory Virtualization, Storage Virtualization, Data Virtualization, Network Virtualization, Virtualization Security Recommendations.	12
	Total	60

Text Book

1. 1.Practical Cloud Security A Guide for Secure Design and Deployment O'reilley Chris Dotson, 2012
2. Cloud Computing Security: Foundations and Challenges, 2nd Edition Securing The Cloud: Cloud Computing Security Techniques and Tactics by Vic (J.R.) Winkler, 2019
3. Ronald L. Krutz, Russell Dean Vines, "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, 2010.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

II Semester	MALWARE ANALYSIS & REVERSE ENGINEERING	L	T	P	C
		3	0	0	3

Course Objectives:

1. To understand the purpose of computer infection program.
2. To implement the covert channel and mechanisms.
3. To test and exploit various malware in open source environment.
4. To analyze and design the famous virus and worms.
5. Understand the Reverse Engineering (RE) Methodology
6. 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 (Four to Six)

		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	K4
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	How to 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
CO1			M	M		
CO2				H	H	
CO3				H	H	
CO4				H	H	
CO5				M	M	
CO6						

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

UNIT	CONTENTS	Contact Hours
UNIT – 1	**Malware Basics**- General Aspect of Computer infection program, Non Self Reproducing Malware, How does Virus Operate, Virus Nomenclature, Worm Nomenclature, Recent Malware Case Studies.	12
UNIT – 2	**Basic Analysis-** Antivirus Scanning, x86 Disassembly, Hashing, Finding Strings, Packed Malware, PE File Format, Linked Libraries & Functions, PE Header File &Section	12

UNIT – 3	**Advanced Static & Dynamic Analysis**-IDA Pro, Recognizing C code constructs, Analyzing malicious windows program, Debugging, OllyDbg, Kernel Debugging with WinDbg, Malware Focused Network Signatures	12
UNIT – 4	**Malware Functionalities-**Malware Behavior, Covert Malware Launch, Data Encoding, Shell code Analysis	12
UNIT – 5	**Reverse Engineering Malware (REM)**: REM Methodology, Resources for Reverse-Engineering Malware (REM) Understanding Malware Threats, Malware indicators, Malware Classification, Examining Clam AV-Signatures	12
	Total	60

Text books:

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

Reference Books:

1. ErciFiliol, “Computer Viruses: from theory to applications”, Springer, 1st edition, 2005.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

II Semester	DIGITAL FORENSICS LAB	L	T	P	C
		0	1	2	2

Course Objectives:

1. To introduce students to the fundamental concepts and principles of computer forensics, including the nature and types of digital evidence.
2. To familiarize students with various forensic tools and techniques used for the collection, preservation, analysis, and presentation of digital evidence.
3. To develop students' practical skills in conducting forensic investigations through hands-on experience with leading forensic software and hardware tools.
4. To provide an understanding of legal, ethical, and procedural aspects associated with forensic investigations and digital evidence handling.

Course Outcomes: At the end of the course, student will be able to (Four to Six)

		Knowledge Level (K)#
CO1	Demonstrate knowledge of core computer forensic concepts and terminology associated with digital investigations.	K2
CO2	Apply appropriate forensic tools to acquire and preserve digital evidence from different types of computing devices and storage media.	K3
CO3	Analyze and interpret digital evidence using forensic software suites to support incident response and legal proceedings.	K4
CO4	Evaluate the legal and ethical considerations relevant to computer forensics and ensure compliance with industry standards and laws.	K5
CO5	Prepare detailed forensic reports and effectively communicate findings to technical and non-technical stakeholders.	K2

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1			M	M		
CO2				H	H	
CO3				H	H	
CO4				M		M
CO5		H		M		
CO6						

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

LIST OF EXPERIMENTS	CONTENTS
EXP– 1	Study of Computer Forensics and different tools used for forensic investigation

EXP –2	How to Recover Deleted Files using Forensics Tools
EXP –3	How to make the forensic image of the hard drive using EnCase Forensics
EXP –4	How to Collect Email Evidence in Victim PC
EXP –5	How to Extracting Browser Artifacts
EXP –6	Find Last Connected USB on your system (USB Forensics)
EXP –7	Live Forensics Case Investigation using Autopsy
EXP –8	Capturing and analyzing network packets using Wireshark
EXP –9	Analyze the packets provided in lab and solve the questions using Wireshark a) What web server software is used by www.uceou.com b) About what cell phone problem is the client concerned? c) How many webservers are running in Apache webserver.
EXP –10	Using Sysinternals tools for Network Tracking and Process Monitoring • Check Sysinternals tools • Monitor Live Processes • Capture RAM • Capture TCP/UDP packets • Monitor Hard Disk • Monitor Virtual Memory • Monitor Cache Memory
EXP –11	Email Forensics • Mail Service Providers • Email protocols • Recovering emails • Analyzing email header
EXP –12	Analyzing data of android mobile using MOBILedit

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

II Semester	PENETRATION TESTING & VULNERABILITY ANALYSIS LAB	L	T	P	C
		0	1	2	2

Course Objectives:

1. To provide practical knowledge of penetration testing methodologies and vulnerability assessment techniques.
2. To develop skills in identifying, exploiting, and analyzing security weaknesses in systems, networks, and applications.
3. To enable learners to recommend effective remediation strategies to enhance overall security posture.

Course Outcomes: At the end of the course, student will be able to (Four to Six)

		Knowledge Level (K)#
CO1	Understand penetration testing methodologies to identify and exploit security vulnerabilities in networks, systems, and web applications	K2
CO2	Use security tools such as Kali Linux, Parrot OS, Nmap, Wireshark, and Metasploit for vulnerability assessment and exploitation.	K2
CO3	Demonstrate exploitation techniques including SQL injection, XSS, CSRF, insecure file handling, and password attacks.	K3
CO4	Analyze network traffic, open ports, and system weaknesses using advanced scanning and packet analysis tools.	K4
CO5	Apply advanced exploitation methods such as rootkits, ARP spoofing, buffer overflow, and tunneling techniques for security testing.	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	-	-	M	H	H	
CO2	-	-	-	H	H	
CO3	-	-	-	H	H	
CO4	-	-	-	H	H	
CO5	-	-	-	H	H	

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

LIST OF EXPERIMENTS	CONTENTS
EXP–1	Implement penetration testing and phases of penetration testing
EXP–2	Make use of different types of tools available in kali and parrot O.S
EXP–3	Practice different SQL injection attacks
EXP–4	Implement and use GHDBC and Microsoft Vulnerabilities (Common

	CVE)
EXP–5	Implement Exploit insecure file handling, upload web shells, deface using upload file mechanism
EXP–6	Perform XSS attacks on client side application
EXP–7	Implement a case on actions on-behalf users by CSRF, Test websites for Clickjacking
EXP–8	Implement port scanning by using NMAP and other tools to find the open ports
EXP–9	Text for wireshark and tcp dumps to analyze various types of packets
EXP–10	Implement Password attacks with methods like Dictionary Files - Key-space Brute Force - Pwdump and Fgdump - Windows Credential Editor (WCE- Exercises - Password Profiling - Password Mutating
EXP–11	Implement metasploit frameworks
EXP–12	Implement Trojan horse root kits backdoors
EXP–13	Practice ARP spoofing and buffer overflow exploitation with ETERCAP ANDSHELL'S
EXP–14	Perform Port Redirection, SSL Encapsulation - Stunnel, HTTP CONNECT Tunneling, Proxy Tunnel, SSH Tunneling.

List of open Source software/learning Websites:

1. https://www.hackthebox.eu/
2. https://practicalpentestlabs.com/
3. https://pentesterlab.com

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CYBER SECURITY COURSE STRUCTURE AND SYLLABUS

III Semester	RESEARCH METHODOLOGY AND IPR	L	T	P	C
		3	0	0	3

Course Objectives:

1. Students will be able to define what constitutes a research problem by identifying gaps, inconsistencies, or limitations in existing knowledge.
2. Students will conduct comprehensive literature reviews to pinpoint unresolved issues or future research directions, synthesizing information to formulate clear research questions.
3.Students will demonstrate the ability to convert broad topics or practical concerns into focused, manageable, and empirically investigable research problems

Course Outcomes: At the end of the course, student will be able to (Four to Six)

		Knowledge Level (K)#
CO1	Identify and formulate research problems, design investigative approaches, and apply appropriate data collection and analysis methods.	K2
CO2	Conduct effective literature reviews, maintain research ethics, and prepare structured technical reports and research proposals.	K3
CO3	Explain the nature and types of Intellectual Property Rights and processes for patenting innovations nationally and internationally.	K2
CO4	Analyze patent rights, licensing processes, technology transfer, and the use of patent databases.	K4
CO5	Evaluate recent developments in IPR, including biological systems, software, and traditional knowledge through case studies.	K5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	H		M			
CO2		H				
CO3			M			M
CO4			M			M
CO5			M			M
CO6						

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

UNIT	CONTENTS	Contact Hours
UNIT – 1	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	12

	collection, analysis, interpretation, Necessary instrumentations	
UNIT – 2	Effective literature studies approaches, analysis Plagiarism, Research ethics, Effective technical writing, how to write report, Paper Developing a Research Proposal, Format of research proposal, a presentation and assessment by a review committee	12
UNIT – 3	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	12
UNIT – 4	Patent Rights: Scope of Patent Rights. Licensing and transfer of technology. Patent information and databases. Geographical Indications.	12
UNIT – 5	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	12
	Total	60

REFERENCES:

(1) Stuart Melville and Wayne Goddard, “Research methodology: an introduction for science & engineering students’”
(2) Wayne Goddard and Stuart Melville, “Research Methodology: An Introduction”
(3) Ranjit Kumar, 2nd Edition, “Research Methodology: A Step by Step Guide for beginners”
(4) Halbert, “Resisting Intellectual Property”, Taylor & Francis Ltd ,2007.
(5) Mayall, “Industrial Design”, McGraw Hill, 1992.
(6) Niebel, “Product Design”, McGraw Hill, 1974.
(7) Asimov, “Introduction to Design”, Prentice Hall, 1962.
(8) Robert P. Merges, Peter S. Menell, Mark A. Lemley, “ Intellectual Property in NewTechnological Age”, 2016.T. Ramappa, “Intellectual Property Rights Under WTO”, S. Chand, 2008.