Koneru Lakshmaiah Education Foundation
(Category - 1, Deemed to be University estd. u/s. 3 of the UGC Act, 1956)
Accredited by **NAAC** as 'A++' ★ Approved by AICTE ★ ISO 9001-2015 Certified
Campus: Green Fields, Vaddeswaram - 522-302, Guntur District, Andhra Pradesh, INDIA
Phone No. 08645 - 350200; www.klef.ac.in; www.klef.edu.in; www.kluniversity.in
Admin Off: 29-36-38, Museum Road, Governorpet, Vijayawada - 520 002. Ph: +91 - 866 : 3500122, 2577715, 2576129.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
Y21-M.TECH-DFCS

Course Code	Course Title	S No	CO No	Description of the course outcome
21CS5121	INTRODUCTION TO CYBER SECURITY	1	CO1	Student should be able to understand security concepts and its impact on data security and application. Students should understand cyber laws and ethics.
		2	CO2	Student should be able to various threats faced by cyber system. Students should be able to understand rolls and responsibility of law enforcement against cybercrime.
		3	CO3	Student should be able to understand malware exhibit the processes involved in malware analysis.
		4	CO4	Students should be able to understand risk analysis and management in the context of cyber security.
		5	CO5	Examine and device a solution for cyber threats to secure cyber system.
21CS5120	SOFTWARE SECURITY	1	CO1	Understand the importance of web architecture and able to list out various levels of security
		2	CO2	Learn and demonstrate various attacks that are occurred in web applications (OWASPTOP10vulnerabilities)
		3	CO3	Differentiate various web application testing techniques and incorporate secure coding practices

		4	CO4	To demonstrate skills needed to deal with common programming errors that lead to most security problems and to learn how to develop secure applications and Summarize on web investigation process P
21CS5122	CLOUD INFRASTRUCTURE & SERVICES	1	CO1	Apply on-demand compute services. Understand IaaS Architectures and Implementation Guidelines.
		2	CO2	Analyse applications and frameworks for data analysis and Content delivery in the cloud
		3	CO3	Analyse Cloud Service Availability, Resiliency, and dynamic scaling
		4	CO4	Use Networking and Security Services. Automate cloud Infrastructure, Deployment, and Management
		5	CO5	Hands-On Cloud Administration. Implement, monitor, and manage important cloud services and components including IaaS and PaaS
21CS5119	MACHINE LEARNING & REINFORCEMENT LEARNING	1	CO1	Apply Machine Learning Techniques such as PCA, LDA, Decision Trees to solve Real World Problems
		2	CO2	Build Bayesian models for solving Classification and Prediction problems
		3	CO3	Inspect a movie recommender system
		4	CO4	Apply Neural Network Algorithm techniques to solve Classification, Prediction problems Build a Q-Learning based model for real world problems
		5	CO5	Implement Machine Learning Techniques using Python Language and develop a small project along with his/her team members.

21IE5149	SEMINAR	**1**	CO5	**The Seminar has to be taken up by the MTech Second Semester students. It is based on independent research in one of the areas opted by the student. In a Seminar, a student should demonstrate his/her ability in finding out the relevant sources, selection, an illustration of logic, and in organizing the information on the topic, gathering the data, processing, analyzing, and summarizing.**
21CS5221	CRYPTOGRAPHY FOR CYBER DEFENSE		CO1	Able to demonstrate the concepts of cryptography.
			CO2	Able to experiment the functionality of cryptographic algorithms.
			CO3	Able to implement the algorithms and explain the strength of the algorithms
			CO4	Able to analyse the security engineering principles in cryptography for cyber defence.
			CO5	able to acquire knowledge on algorithms and their procedures for maintaining the security for cyber defence using tools and technologies.
21CS5222	MALWARE ANALYSIS & REVERSE ENGINEERING		CO1	Understand Malware types and malware fundamentals.
			CO2	Understand Malware Reverse Engineering techniques.
			CO3	Understand static and dynamic Malware Analysis by using different tools and techniques.
			CO4	Apply Malware Analysis on malicious Microsoft Office (Word, Excel, PowerPoint) and Adobe PDF documents
			CO5	Student should be able to acquire knowledge on Malware and their Analysis, Reverse Engineering procedures using different tools and technologies for Malware Analysis.
			CO1	Understand Incident Response concepts.

			CO2	Understand the functionality of Incident Response and Incident categories and handling.
21CS5223	CYBER INCIDENT RESPONSE & RESILIENCE		CO3	Exhibit the processes involved in Incident Handling Process
			CO4	Analyze and understand Incident Response Team Members Roles and Responsibilities.
			CO5	Express the dependencies in incident Response team.
21CS5224	CYBER LAW, GOVERNANCE & COMPLIANCE		CO1	Student should be able to Understand the Concepts of Cyber Ethics and cyberlaw importance
			CO2	Student should be able to Identify the various IT Acts ITA2000,ITAA 2008..
			CO3	Student should be able to protection of intellectual property Rights.
			CO4	Student should be able to investigate the Cyber Frauds.
			CO5	Student should be able to Acquire knowledge on CYBERLAW,GOVERNANCE& COMPLIANCE .
21IE5250	Term Paper		CO5	The term paper has to be taken up by the MTech Second Semester students. It is based on independent research in one of the areas opted by the student. In a term paper, a student should demonstrate his/her ability in finding out the relevant sources, selection, an illustration of logic, and in organizing the information on the topic, gathering the data, processing, analyzing, and summarizing.
21IE6050	Dissertation		CO5	The Project has to be taken up by the MTech Second Semester students. It is based on independent research in one of the areas opted by the student. In a project research paper, a student should demonstrate his/her ability in finding out the relevant sources, selection, an illustration of logic, and in organizing the information on the topic, gathering the data, processing, analyzing, and summarizing.
ELECTIVE-1				

21CS51I1	Mobile Device Threats & Investigation		CO1	Familiarize with the issues and technologies involved in designing a wireless and mobile system that is robust against various attacks.
			CO2	Gain knowledge and understanding of the various ways in which wireless networks can be attacked and trade-offs in protecting networks.
			CO3	Have a broad knowledge of the state-of-the-art and open problems in wireless and mobile security, thus enhancing their potential to do research or pursue a career in this rapidly developing area.
			CO4	Learn various security issues involved in cloud computing.
				Learn various security issues related to GPRS and 5G.
21CS51I2	Fundamentals of E-Discovery		CO1	Become familiar with the e-discovery rules and other sources of e-discovery law
			CO2	Become familiar with e-discovery ethical issues and e-discovery best practices
			CO3	Learn how to apply their knowledge to resolve typical and somewhat more complex e-discovery problems
			CO4	Acquire basic knowledge and skill in using e-discovery software
21CS51I3	Fuzzy sets and Fuzzy Logic		CO1	Understand basic knowledge of the fuzzy sets, operations and their properties
			CO2	Understand the fundamental concepts of Fuzzy functions and Fuzzy logic
			CO3	Apply the concepts of Fuzzy sets in decision making.
			CO4	Apply the concepts of Fuzzy logic and fuzzy sets in applications.
			CO1	Understand the steps of forensics process.

21CS51I4	Digital Forensics		CO2	Apply forensics analysis on different hard drives and analyze the file systems.
			CO3	Analyze the various components and data in mobile phone for evidence.
			CO4	Analyze windows registry and the various anti forensics techniques.
			CO5	Create a virtual lab and experiment forensics expts based on the 5 stages of forensics process.
ELECTIVE-2				
21CS51J1	Introduction to Big Data Analytics		CO1	Student should be able to Understand the Overview of the term Big Data and their Evalution
			CO2	Student should be able to come across different types of databases, differentiate NOSQL, SQL
			CO3	Student should able to Understand Analytics in data.
			CO4	Student should able to Illustrate different tools in unstructured data.
21CS51J2	Social Media Forensics		CO1	Understand open-source intelligence and how to utilize it.
			CO2	Analyze online cyber investigations and intelligence gathering on the Dark Web.
			CO3	Apply social networking searching and monitoring
			CO4	Investigate criminal groups on social media and understand the legal fundamentals of cyber investigations.
			CO1	Identify the key characteristics and problems in the area of cyber-security of critical infrastructure

21CS51J3	Critical Information Infrastructure Security		CO2	Apply research methods which includes survey, experiments, and articulation of research problems in this area, and methods for finding solutions to selected problems
			CO3	Present in written and/or verbal form key findings in the specific subject area of the course from contemporary research papers.
			CO4	Analyze and identify research verticals in the specific domain area of cyber-security of critical infrastructure.
ELECTIVE-3				
21CS52K1	Infrastructure Attacks and Defense		CO1	Understand the concept of vulnerabilities, attacks and protection mechanisms
			CO2	Analyze and evaluate software vulnerabilities and attacks on databases and operating systems
			CO3	Understand and explain various security solutions for Web and Cloud infrastructure
			CO4	Understand, and evaluate different attacks on Open Web Applications and Web services
			CO5	Design appropriate security policies to protect infrastructure components
21CS52K2	Software Vulnerability Analysis and Resilience		CO1	Understand how to exploit a program and different types of software exploitation techniques
			CO2	Understand the exploit development process
			CO3	Investigate various vulnerabilities in closed-source applications
			CO4	Design their own exploits for vulnerable applications
			CO5	Apply and analyse the designed exploits in real time applications

21CS52K3	Parallel & Cloud Computing		CO1	Articulate the main concepts, key technologies, strengths, limitations of parallel and cloud computing and the possible applications for state-of-the-art cloud computing.
			CO2	Identify the architecture and infrastructure of parallel and cloud computing, including cloud delivery and deployment models.
			CO3	Analyze the core issues of parallel and cloud computing such as security, privacy, and interoperability.
			CO4	Identify problems and analyze various cloud computing solutions.
			CO5	Evaluate various cloud computing solutions.
21CS52K4	Cloud Security		CO1	Understand the principles of cryptography and Apply various cryptographic algorithms
			CO2	Analyze various security issues and system vulnerabilities in virtualization
			CO3	Analyze the technologies for virtualization based security enhancements
			CO4	Analyze legal and Compliance issues and examine modern security standards
			CO5	Interpret various standerds to overcome critical platform security issues
ELECTIVE-4				
	Applied Cryptography and		CO1	Understand the main concepts of Modern Cryptography and steganography.
			CO2	Apply various cryptographic and steganography algorithms in a real time approaches and analyse the working methodologies and key properties.

21CS52L1	Applied Cryptography and Steganography		CO3	Evaluate functionality, security and performance properties of cryptography and steganography methods used as components of complex security solutions
			CO4	Analyse the impact of errors or different designs of cryptography and steganography algorithms and protocols
21CS52L2	Software Modeling		CO1	Student should be able to uunderstand the cconcepts of Basics of Software Engineering
			CO2	Student should be able to understand the functionality of Unified Modelling Language.
			CO3	Student should be able to analyze the feasibility by performing Root Cause Analysis, Reverse estimation and by tracking.
			CO4	Student should be able to Acquire knowledge on programming languages
21CS52L3	Digital Image Processing		CO1	To understand the fundamental concepts of Digital Image Processing
			CO2	To understand the pre-processing process of remote sensing data
			CO3	To understand basic image processing operations
			CO4	To understand image classification techniques
			CO5	To apply digital image Processing techniques
21CS52L4	Programming For Smart Contracts		CO1	Understanding Ethereum blockchain and using wallet for interacting with network
			CO2	Learn and use solidity programming language to build smart contracts
			CO3	Building advanced smart contracts with various test setups and try-catch assertions.
			CO4	Build interactive front end for smart contracts and use Contracts design patterns.

			CO5	Implement lab experiments through project-based learning on building smart contracts