SYLLABUS

DR VISHWANATH KARAD
MIT - WORLD PEACE UNIVERSITY

FACULTY OF ENGINEERING AND TECHNOLOGY

SCHOOL OF COMPUTER ENGINEERING AND TECHNOLOGY

B. TECH. COMPUTER SCIENCE AND ENGINEERING (CYBERSECURITY AND FORENSICS)

BATCH: 2021 – 2025

4/8/23

COURSE STRUCTURE

Course Code	CET3003B			
Course Category	Professional Core			
Course Title	Full Stack Development			
Total Teaching Hrs. and Credits	Lectures	Tutorial	Laboratory	Credits
	--	--	04	02

Pre-requisites:

- Principles of Programming Languages
- Computer Networks

Co-requisite

1. Database Management Systems

Course Objectives:

2. To understand the basics of the web development.
3. To acquire skills for developing web applications using front end technologies.
4. To learn application development using back end technologies.
5. To study testing and deployment processes for the real world web-based applications.

Course Outcomes:

On completion of course, students should be able to

1. Develop web applications using HTML and CSS.
2. To select and apply appropriate front end technologies for responsive web application development
3. To design and develop web application using appropriate backend technologies
4. Test and deploy real world web-based application on different platforms

Course Contents:

Laboratory Exercises:

1. Responsive web design using HTML5, CSS and Bootstrap
2. Web application using sessions, cookies and form validation
3. Interactive front end application using React components, States and Props, Class, Events.
4. Responsive front end application using React Lists and Portals, Error Handling, Routers and style with React CSS
5. Responsive web design using Express Framework and MongoDB
6. Mini Project

Learning Resources:

Text Books:

1. Ralph Moseley & M. T. Savaliya(2007), "Developing Web Applications", Wiley publications.
2. Eric Bush (2016), Full-Stack JavaScript Development, ISBN:9780997196603

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Reference Books:

1. Hands-On Full Stack Web Development with Aurelia : Develop modern and real-time web applications with Aurelia and Node.js by Diego Jose Arguelles Rojas, Erikson Haziz Murrugarra Sifuentes, 2018, Packt
2. Modern Full-Stack Development Using TypeScipt, React, Node,js, Webpack, Docker by Zammetti, Frank
3. Achyut Godbole & Atul Kahate, "Web Technologies: TCP/IP to Internet Application Architectures", McGraw Hill Education publications, ISBN, 007047298X, 9780070472983
4. Full-Stack JavaScript Development Develop, Test and Deploy with MongoDB, Express, Angular and Node on AWS Eric Bush, Maura van der Linden, 2016

Supplementary Reading:

- https://www.geeksforgeeks.org/how-to-become-a-full-stack-web-developer-in-2021/
- https://www.hackerearth.com/blog/full-stack/
- https://careerfoundry.com/en/blog/web-development/what-is-a-full-stack-web-developer/
- https://www.upgrad.com/blog/how-to-become-a-full-stack-developer-part-1/

Web Resources:

- The Full Stack Developer Your Essential Guide to the Everyday Skills Expected of a Modern Full Stack Web Developer by Chris Northwood, Apress, 2018
- Full Stack Javascript by Azat Mardan Apress Publication, 2015

Web links:

- https://www.pmi.org/learning/library/agile-project-management-scrum-6269
- https://www.w3schools.com/whatis/whatis_fullstack.asp
- https://www.geeksforgeeks.org/what-is-full-stack-development/

MOOCs:

- https://www.tutorialspoint.com/the_full_stack_web_development/index.asp
- https://prutor.ai/fullstackdeveloperonlinetraining/
- https://www.udacity.com/course/full-stack-web-developer-nanodegree--nd0044
- https://nptel.ac.in/courses/106106156

Pedagogy:

- PowerPoint Presentation
- Video Lectures
- Flipped Classroom Activity
- Open source Tools
- Project Based Learning

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Assessment Scheme:
Laboratory Continuous Assessment: 100 Marks

Practical Performance	Additional implementation/ Content beyond syllabus	Active Learning	Mini-project	Oral
30	10	10	40	10

Syllabus - Laboratory:

Lab	Assignment Statement	Workload in Hrs. Lab
1	Develop responsive web design using HTML5, containing a form. Style the pages using CSS, Use of tag selector, class selector and id selectors. Use Inline, Internal and External CSS,Apply Bootstrap CSS	04
2	Develop a web application using javascript to implement sessions, cookies, DOM. Perform validations such as checking for emptiness, only numbers for phone number, special character requirement for password, regular expressions for certain format of the fields etc. Use the mySQL database.	04
3	Design an interactive front end application using React by implementing templating using components, States and Props, Class, Events. It must be responsive to scale across different platforms.	04
4	Enhance web page developed in earlier assignment by rendering Lists and Portals, Error Handling, Routers and style with React CSS also make it a responsive design to to scale well across PC, tablet and Mobile Phone	04
5	Develop a responsive web design using Express Framework to perform CRUD operations and deploy with Node JS. use MongoDB.	06
6	Mini Project	08
	Total	**30**

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Dr. Dinesh Seth
Dean

COURSE STRUCTURE

Course Code	**CET4029B**			
Course Category	**Professional Elective-I (PE)**			
Course Title	**Cyber Threat Modeling**			
Total Teaching Hrs and Credits	**Lectures**	**Tutorial**	**Laboratory**	**Credits**
	3	**--**	**2**	**3+1=4**

Pre-requisites

- Information Security, Linux essentials and networking basics

Course Objectives:

1. To study threat modeling while designing a system
2. To understand the concept of threat modeling methodologies
3. To learn the approaches used by adversaries to attack the system infrastructure
4. To learn various aspects of threat modeling in cyber security

Course Outcomes:

On completion of course, students should be able to

1. Understand the vulnerabilities to a computer and its network
2. Develop skills to learn securing Internet connected computing devices
3. Identify threats and potential attack points in a computer and networking infrastructure
4. Understand and apply threat modeling in securing various systems

Course Contents:

1. Cyber Attacks and Threats
2. System Threat Modeling
3. Processing and Managing Threats
4. Trade-Off s of Addressing Threats
5. Privacy Tools

Laboratory Exercises:

1. Learn how to scan a host using Nmap and understand the results.
2. Learn how to test a website for an XXS vulnerability – Cross site scripting.
3. Learn how to automate SQL injection using SQLmap.
4. Learn how to run a comprehensive vulnerability scan with Nessus.
5. Learn how to conduct a manual SQL injection attack.
6. Learn how to capture packets using tcpdump.
7. Learn how to use hping for security auditing and the testing of networking devices.
8. Learn how to use the Nslookup command to gather DNS information on a target site.
9. Learn how to use Scanless to anonymously scan a target.
10. Learn how to use macchanger to spoof your MAC address.

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Learning Resources:

Text Books:

1. Adam Shostack, 'Threat Modeling - Designing for Security', Wiley
2. Izar Tarandach & Matthew J. Coles, 'Threat Modeling A Practical Guide for Development Teams', O'Reilly
3. James Graham, Richard Howard, Ryan Olson, 'Cyber Security Essentials', CRC Press, Taylor & Francis Group

Reference Books:

1. Zane Pokorny Foreword by Christopher Ahlberg, 'The Threat Intelligence Handbook - Moving Toward a Security Intelligence Program', CyberEdge Press, 2nd Edition
2. Florian Skopik, 'Collaborative Cyber Threat Intelligence – Detecting and Responding to Advanced Cyber Attacks at the National Level', CRC Press Taylor & Francis Group, 2018
3. James Michael Stewart, Mike Chapple, Darril Gibson, 'CISSP Certified Information Systems Security Professional Study Guide', Wiley, 2015, 7th Edition
4. Thomas A. Johnson, 'CYBER- SECURITY Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare', CRC Press Taylor & Francis Group, 2017

Supplementary Reading:

Web Resources:

https://nptel.ac.in/courses/106106129
https://www.udemy.com/course/cybersecurity-from-beginner-to-expert/
https://www.udemy.com/course/network-security-course/

Web links:

https://www.101labs.net/comptia-security/lab-2-nmap/
https://www.101labs.net/comptia-security/
https://engineering.purdue.edu/kak/compsec/NewLectures/
https://matthewomccorkle.github.io/

MOOCs:

https://www.coursera.org/professional-certificates/ibm-cybersecurity-analyst

Pedagogy:

1. Power Point Presentation
2. Two Teacher Method
3. Video Lectures
4. Flipped Classroom Activity
5. Group Discussion
6. Chalk and Board

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Assessment Scheme:
Class Continuous Assessment: 30 Marks

Assignments	Mid Term Exam	Case study
05 Marks	15 Marks	10 Marks

Laboratory Continuous Assessment: 30 Marks

Practical	Oral
15 Marks	15 Marks

Term End Examination: 40 Marks

Syllabus: Theory

Module No.	Contents	Workload in Hrs
		Theory
1	**Cyber Attacks and Threats** Attacker techniques and motivation, How Hackers Cover Their Tracks, Fraud Techniques, Threat Infrastructure, Exploitation, Techniques to Gain a Foothold, Misdirection, Reconnaissance, and Disruption Methods	09
2	**System Threat Modeling** System Modeling Types, Building System Models, Properties of a Good System Model, A Generalized Approach to Threat Modeling, Learning to Threat Model, Threat Modeling on Your Own, Checklists for Diving In Threat Modeling, Brainstorming Your Threats, Structured Approaches to Threat Modeling	09
3	**Processing and Managing Threats** Starting the Threat Modeling Project, Digging Deeper into Mitigations, Tracking with Tables and Lists, Scenario-Specific Elements of Threat Modeling	09
4	**Trade-Offs of Addressing Threats** Classic Strategies for Risk Management, Selecting Mitigations for Risk Management, Threat-Specific Prioritization Approaches, Testing Threat Mitigations, Process Aspects of Addressing Threats	09
5	**Privacy Tools** Understanding STRIDE and its need, Spoofing Threats, Tampering Threats, Repudiation Threats, Information Disclosure Threats, Denial-of-Service Threats, Elevation of Privilege Threats, Extended Example: STRIDE Threats against Acme-DB	09

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Laboratory:

Module No.	Contents (Any 8)	Workload in Hrs
		Lab
1	Learn how to scan a host using Nmap and understand the results.	04
2	Learn how to test a website for an XXS vulnerability – Cross site scripting.	04
3	Learn how to automate SQL injection using SQLmap.	04
4	Learn how to run a comprehensive vulnerability scan with Nessus.	04
5	Learn how to conduct a manual SQL injection attack.	02
6	Learn how to capture packets using tcpdump.	02
7	Learn how to use hping for security auditing and the testing of networking devices.	02
8	Learn how to use the Nslookup command to gather DNS information on a target site.	02
9	Learn how to use Scanless to anonymously scan a target.	02
10	Learn how to use mac changer to spoof your MAC address.	02

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Dr. Dinesh Seth
Dean

COURSE STRUCTURE

Course Code	CET4004B			
Course Category	Professional Elective I (D)			
Course Title	Wireless and Mobile Device Security			
Teaching Scheme and Credits	Lectures	Tutorial	Laboratory	Credits
Weekly load hrs.	3	-	2	3+1=4

Pre-requisites:

- Basics of Computer Networks,
- Basics of Information & Cyber Security

Course Objectives:

Knowledge:

i. To understand wireless networks technologies and applications
ii. To study Ad-Hoc networks architecture and challenges
iii. To know Sensor networks architecture and applications
iv. To understand basic security needs and issues in wireless networks
v. To understand mobile device security architecture and security dynamics

Skills:

i. This course will give you detailed insights of how Wireless Network, Wireless Ad-hoc Network, Mobile Device configuration performance measures works and security aspects of it.
ii. This course gives understanding of how to design and configure your own network.

Attitude:

i. As the designing and configuration is required, in this case, to deploy the network as well as provide various security aspects to the mobile device so that the intended output can be achieved.

Course Outcomes:

After completion of this course students will be able to

1. Compare different wired and wireless technologies
2. Simulate and analyze wireless Ad-Hoc networks for different protocols
3. Analyze the security threats in wireless sensor networks
4. Devise and Configure wireless security in Wi-Fi networks
5. Configure or Program security needs in mobile devices

Course Contents:

1. Introduction Wireless Networks
2. Ad-Hoc Wireless Networks
3. Wireless Sensor Networks
4. Security in Wireless Networks
5. Mobile device security aspects

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Learning Resources:

Text Books:

1. C. Siva Ram Murthy, B.S. Manoj, "Adhoc Wireless Networks Architectures and Protocols", PHI, ISBN - 9788131706885, 2007.
2. Nekoley Elenkov, "Android Security internals", No Starch Press, ISBN-10: 1-59327-581-1 ISBN-13: 978-1-59327-581

Reference Books:

1. KiaMakki, Peter Reiher, "Mobile and Wireless Network Security and Privacy ", Springer, ISBN 978-0-387-71057-0, 2007.
2. Hakima Chaouchi, Maryline Laurent-Maknavicius , "Wiress and Mobile Networks Security", Wiley publication, ISBN 978-1-84821-117-9
3. Noureddine Boudriga, "Security of Mobile Communications", ISBN 9780849379413, 2010.
4. Kitsos, Paris; Zhang, Yan, "RFID Security Techniques, Protocols and System-On-Chip Design", ISBN 978-0-387-76481-8, 2008.
5. Johny Cache, Joshua Wright and Vincent Liu," Hacking Wireless Exposed: Wireless Security Secrets & Solutions ", second edition, McGraw Hill, ISBN: 978-0-07-166662-6, 2010
6. Tim Speed, Darla Nykamp, Mari Heiser, Joseph Anderson, Jaya Nampalli, "Mobile Security: How to Secure, Privatize, and Recover Your Devices", Copyright © 2013 Packt Publishing, ISBN 978-1-84969-360-8

Supplementary Reading:

Web Resources:

1. http://whatis.techtarget.com/definition/mobile-security
2. http://techgenix.com/security/mobile-wireless-security/

Weblinks:

1. https://en.wikipedia.org/wiki/Mobile_security

MOOCs:

1. https://www.ntnu.edu/studies/courses/TTM4137#tab=omEmnet
2. http://nptel.ac.in/courses/106105160/37
3. https://www.eccouncil.org/
4. https://www.csoonline.com/article/2122635/mobile-security/wireless-security--the-basics.html

Pedagogy:

1. Power Point Presentation
2. White-board / Pen
3. Demos of Security tools
4. Online Quizzes
5. Video Clips
6. Oral Questions and Answers.

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Assessment Scheme:

Class Continuous Assessment (CCA): 30 Marks

Mid Term	Component 1 (Active Learning)	Component 2
15 Marks	10 Marks	05 Marks

Laboratory Continuous Assessment (LCA): 30 Marks

Practical Performance	Active learning / Mini Project/Additional implementation/ On paper design	End term practical /oral examination
10 Marks	10 Marks	10 Marks

Term End Examination: 40 Marks

Syllabus: Theory

Module No.	Contents	Workload in Hrs. Theory
1	**Introduction Wireless Networks** Introduction to Wireless LAN, PAN, MAN, WAN- Technical issues, Network Architecture, Advantages. Overview of IEEE 802.11, 802.15, 802.16- Architecture, Features and applications. Mac protocols- CSMA-CA, Hidden station and exposed station problems. Mobile cellular networks - Generations overview, features and applications. Cellular architecture system, Handoffs and Handover. Introduction to 4G and 5G.	09
2	**Ad-Hoc Wireless Networks** Ad-Hoc Wireless Networks: Properties and Challenges, Applications and Issues in MAC design in Ad-Hoc wireless networks, Design Goals of MAC. Routing design issues in Ad-Hoc networks. Classifications of Routing protocols, Table Driven: DSDV, WRP, CGR. On Demand: AODV and DSR, TORA protocol, Introduction to Multicast Routing Protocols	09 -
3	**Wireless Sensor Networks** Introduction, Applications, Challenges in design issues in sensor networks, Architecture of sensor networks: Layered Architecture, Clustered Architecture, Overview of Data Dissemination techniques, Introduction to Data Gathering techniques. Overview of Positioning, Localization and Synchronization in Sensor networks, LoRa WANs, RFID technologies.	09
4	**Security in Wireless Networks** Security in Ad Hoc Wireless Networks, Network Security Requirements, Issues and Challenges in Security Provisioning, Network Security Attacks	09

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

	and other attacks, Key Management in Adhoc Wireless Networks, Requirements of a Secure Routing Protocol for Ad Hoc Wireless Networks, Overview of WiFi security, Issues in WiFi Security, Access Point security, Authentication in Wireless networks, Security in IPV4 and IPv6 protocols.	
5	**Mobile Device Security** Introduction to Device management and security, Mobile device architecture: Android OS, macOS, Details of Device Security: Android Security Model, macOS Security Model, Device Permissions Disk Encryption, Screen Security, Secure USB Debugging, Overview of various Mobile Malware, Network Attacks, Mobile malware defences: Advantages and disadvantages, protect against Mobile Malware, protect against identity theft, protect against Mobile ioS Security- iOS security overview-pairing, back up, configuration, introducing app security, blocking access, key bags& key chains.	09

Laboratory:

Lab No.	Contents	Workload in Hrs
		Lab
1	Install and Configure Network Simulator tool such as Network Simulator 2 or NetSim or QualNet and study its components and eco system.	02
2	Write a program to simulate two nodes wireless network. You may use NetSim or NS2 or QualNet for this experiment.	02
3	Write a program to simulate routing in mobile Ad-Hoc network with multiple nodes. You may use NetSim or NS2 or QualNet for this experiment.	02
4	Study the security permissions for applications in android phones. Either demonstrate Android security permission configurations or Write the android app to demonstrate permissions usage control in android phones.	02
5	Write an android program to encrypt and decrypt text file. Use Bouncy castle library API or Java cryptography API.	02
6	Write a program for user authentication application in Java or Python. Send OTP (one time passwords) to your mobile phones from this application and validate that OTP. It should tell of OTP is correct or wrong. Also add timing restriction in the application.	02
7	Configure access point and manage the access control for security. Access point is a networking hardware device that allows a Wi-Fi device to connect to a wired network.	02
8	Study, comparison and configuration of different types of Access points routers such CISCO, TP Link, DLink, Link Sys, NetGear. Study Technical specification of such a Wi-Fi router.	02

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

9	Install, Configure and Demonstrate any one Wi-Fi traffic analyzer using sniffing tools such as WireShark, airCrack, AirSnort, etc.	02
10	Consider Android and iPhone device. Analyse, experiment all aspects of device security in these mobile devices. Compare and contrast pros and cons.	02
11	Write an Android Application to create secured mobile wallet with cryptographic algorithms	02
12	Home Automation (Monitoring and Control) with ZigBee Devices: Scenario Description: ZigBee allows small, low-cost devices to quickly transmit small amounts of data such as temperature readings for thermostats, on/off requests for light switches, or keystrokes for a wireless keyboard. The scenario showsan application of ZigBee technology for Home Automation. It demonstrates the monitoring and control capability that can be achieved with ZigBee.	02

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Dr. Dinesh Seth
Dean

COURSE STRUCTURE

Course Code	CET4030B			
Course Category	Professional Elective - I			
Course Title	Incident Response and Malware Analysis			
Total Teaching Hrs. and Credits	Lectures	Tutorial	Laboratory	Credits
	03	--	02	3+1=4

Pre-requisites

- Basic knowledge of computer networking and operating systems
- Familiarity with programming concepts and languages (e.g., Python, C)
- Understanding of computer security concepts and technique

Course Objectives:

1. To introduce students to the concepts and principles of incident response and malware analysis.
2. To provide students with the skills and knowledge needed to effectively respond to security incidents and analyze malware.
3. To familiarize students with the tools and techniques used in incident response and malware analysis, including those used to detect, contain, and eradicate attacks.
4. To help students develop critical thinking skills related to incident response and malware analysis, including the ability to assess risks and make informed decisions.
5. To provide students with an understanding of the legal and ethical issues related to incident response and malware analysis, including privacy concerns and compliance with relevant regulations and policies.
6. To expose students to real-world case studies and scenarios, allowing them to apply the concepts and techniques learned in class to practical situations.

Course Outcomes:

On completion of course, students should be able to

1. Students will be able to identify and respond to security incidents in a timely and effective manner.
2. Students will be able to analyze malware and identify its characteristics, behavior, and impact on a system or network.
3. Students will be able to use various tools and techniques to detect, contain, and eradicate attacks, including those used for network analysis, memory forensics, and malware analysis.
4. Students will be able to assess the risks associated with different types of security incidents and make informed decisions about how to respond to them.
5. Students will have an understanding of the legal and ethical issues related to incident response and malware analysis, and be able to apply this knowledge to real-world scenarios.
6. Students will be able to communicate effectively about incident response and malware analysis, including presenting findings and recommendations to technical and non-technical audiences.
7. Students will be able to apply the concepts and techniques learned in class to practical situations, including through the analysis of real-world case studies.

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
Date 08 JUN 2023

Course Contents:

1. Introduction to Incident Response
2. Incident Response Preparation and Execution
3. Introduction to Malware Analysis
4. Malware Analysis Techniques and Tools
5. Incident Response and Malware Analysis Case Studies

Learning Resources:

Text Books:

1. "Incident Response & Computer Forensics, Third Edition" by Jason Luttgens, Matthew Pepe, and Kevin Mandia
2. "Practical Malware Analysis: A Hands-On Guide to Dissecting Malicious Software" by Michael Sikorski and Andrew Honig

Reference Books:

1. "Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code" by Michael Hale Ligh, Steven Adair, Blake Hartstein, and Matthew Richard
2. "Windows Internals, Part 1: System architecture, processes, threads, memory management, and more" by Mark Russinovich, David Solomon, and Alex Ionescu

Pedagogy:

1. Power Point Presentation
2. Two Teacher Method
3. Video Lectures
4. Flipped Classroom Activity
5. Group Discussion
6. Chalk and Board

Assessment Scheme:

Class Continuous Assessment (CCA): 30 Marks

Mid Term	Component 1 (Active Learning)	Component 2
15 Marks	10 Marks	05 Marks

Laboratory Continuous Assessment (LCA): 30 Marks

Practical Performance	Active learning / Mini Project/Additional implementation/ On paper design	End term practical /oral examination
10 Marks	10 Marks	10 Marks

Term End Examination: 40 Marks

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Dr. Dinesh Seth
Dean

Syllabus: Theory

Module No.	Contents	Workload in Hrs. Theory
1	**Unit 1: Introduction to Incident Response** **Overview of Incident Response and its importance**, Definition of Incident Response, Reasons why Incident Response is important, Common types of incidents that require a response, **Key stakeholders in Incident Response**, Roles and responsibilities of key stakeholders, How stakeholders interact during an incident, **Incident Response phases and key activities**, Overview of the Incident Response phases (Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned), Key activities in each phase, **Incident Response frameworks (e.g., NIST, SANS)**, Overview of popular Incident Response frameworks, How to use Incident Response frameworks to guide Incident Response activities.	09
2	**Unit 2: Incident Response Preparation and Execution** **Incident Response Plan (IRP) creation** What an IRP is and why it is important, How to create an effective IRP, Best practices for testing and validating an IRP **IRP testing, validation, and updating** Different methods of testing an IRP, Importance of validation and updating an IRP. **Incident Response Team (IRT) formation and roles** What an IRT is and why it is important, How to form an effective IRT, Roles and responsibilities of IRT members **Incident identification and triage** How to identify an incident, Triage process for prioritizing incidents **Containment and eradication of incidents** Techniques for containing an incident, Methods for eradicating an incident **Data collection, preservation, and analysis** Importance of data collection and preservation, Methods for collecting and preserving data, Techniques for analyzing data **Communication and collaboration during Incident Response** Importance of effective communication during Incident Response, Techniques for communicating with stakeholders, Strategies for collaborating with stakeholders **Recovery and post-incident activities** Techniques for restoring normal operations, Best practices for conducting post-incident activities	09

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date.....

3	**Unit 3: Introduction to Malware Analysis** **Overview of Malware and its types** **Definition of Malware** **Common types of Malware (e.g., Virus, Worm, Trojan)** Malware analysis techniques and tools, Overview of Malware analysis techniques (e.g., static and dynamic analysis) **Popular Malware analysis tools (e.g., IDA Pro, Ollydbg, Process Hacker, Wireshark)** Malware analysis phases (e.g., static and dynamic analysis), Overview of Malware analysis phases (e.g., static and dynamic analysis),Key activities in each phase	09
4	**Unit 4: Malware Analysis Techniques and Tools** **Static Analysis Techniques** Strings Analysis, File Analysis, Packer Detection and Unpacking **Dynamic Analysis Techniques** Sandboxing, Debugging, Memory Analysis **Malware Reverse Engineering** Introduction to Reverse Engineering, Assembly Language Basics Disassembly Techniques, Dynamic Analysis in Reverse Engineering **Malware Analysis Tools (e.g., IDA Pro, Ollydbg, Process Hacker, Wireshark)** Overview of popular Malware Analysis Tools, How to use Malware Analysis Tools effectively	09
5	**Unit 5: Incident Response and Malware Analysis Case Studies** **Real-world case studies on Incident Response and Malware Analysis** Analysis of real-world incidents and Malware attacks **Analyzing the tools and techniques used in the case studies** How the Attack attack was executed, The tools and techniques used by the attacker, The impact of the attack on the target organization **How Incident Response and Malware Analysis were used to contain and eradicate the attacks** The Incident Response and Malware Analysis techniques used to contain and eradicate the attack, The lessons learned from the case studies	09

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Dr. Dinesh Seth
Dean

Laboratory Syllabus:

Module No.	Laboratory	Workload in Hrs
1	Write a standard Incident Response report based on the frameworks (e.g., NIST, SANS).	04
2	Prepare a Data collection framework for an incident based on memory dump collection for Microsoft Windows and Unix/Linux based systems using a tool.	04
3	How to decide on a Malware Analysis methodology for an incident. Implement the same with a tool.	04
4	Identify and list potential sources of incident response data on a Microsoft Windows operating system. Explain the purpose and potential evidence that may be found in the following areas; NTFS/File System, Prefetch, Event logs, Scheduled tasks, and the Windows registry.	04
5	From a given infected application, how is potential forensic evidence data derived from the applications. Analyze web browser user data, identify and list the potential vulnerabilities..	04
6	Use a tool to perform Live data collection in a Client-Server Environment.	04
7	Perform Static and Dynamic Malware Analysis with the help of a tool.	04
8	Case Study, go through a analysis report and comment on what more can be done to identify potential problems that may have been left out.	04

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Dr. Dinesh Seth
Dean

COURSE STRUCTURE

Course Code	CET4031B			
Course Category	Professional Elective			
Course Title	Identity Management			
Total Teaching Hrs. and Credits	Lecture	Tutorial	Laboratory	Credits
	03	--	02	3+1=4

Pre-requisites

- Information and Cyber Security

Course Objectives:

1. Knowledge

(i) To understand the basics of Identity and Access Management in Security
(ii) To acquaint with Access Control Models.

2. Skills

(i) To comprehend the importance of Identity and Access Management Lifecycle and Transformation in security planning and contingencies.

(ii) To use Access Control Models and protect data from Access Control Attacks

3. Attitude

(i) To explore critical understanding of various IAM Tools and its use.
(ii) To implement Identity and Access Management Protocols

Course Outcomes:

On completion of course, students will be able to

1. Explore different approaches for implementing effective IAM
2. Evaluate the concepts and principles of Zero Trust as they relate to Identity Management and Access Controls, including the cultural aspects of moving to a 'password-less' environment.
3. Outline various access management and guidance standards
4. Analyze how to manage various processes in organizations and Identify different types of provisioning in organizational processes
5. Evaluate the impact of technology on the evolution of IAM

Course Contents:

1. Identity and Access Management Concepts
2. Access Management Models
3. Organizational Processes, Governance, IAM Guidance and Standards
4. Cloud Services and IAM Implementation
5. Identity and Access Management Technologies

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Dr. Dinesh Seth
Dean

Laboratory Exercises:

1. Working with Windows Server system and Managing Windows Accounts and Organizational Units.
2. Demonstration on Managing Identities in a Digital World.
3. Installation, Configuration and Managing Identity and access in Microsoft 365.
4. Demonstration on ensuring strong authentication and configuring multifactor authentication
5. Working with Active Directory Services and Extending on-premises Active Directory (AD) to Azure AD
6. Implementing SSO in Azure for Office 365 and SaaS applications
7. Authenticating with Amazon IAM roles
8. Implementing Single Sign-On (SSO), Interoperating via open industry standards, federated logon and claims and Applying Kerberos identities in a domain.
9. Demonstrating On-premises and cloud-based identity management
10. Exploring identities in Kerberos tickets and AD attributes. Also Identifying identities in SQL databases
11. Demystifying MIM 2016
    - Importing identities from Connected Data Source CDS into Connector Space CS
    - Synchronizing identities into Metaverse MV
    - Managing identities and rules with the SharePoint MIM Portal

Learning Resources:

Text Books:

1. Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution by Morey J. Haber, Darran Rolls
2. Identity and Access Management by Ertem Osmanoglu, Publisher(s): Elsevier Science, Syngress, ISBN: 9780124104334
3. Identity and Access Management A Complete Guide - 2020 Edition by Gerardus Blokdyk

Reference Books:

1. Identity Management: A Primer By Graham Williamson, David Yip, Ilan Sharoni, Kent Spaulding, Copyright © 2009 MC Press Online, LP, ISBN-13 : 978-1583470930
2. Identity Management: Concepts, Technologies, and Systems (Information Security & Privacy) by Elisa Bertino, Kenji Takahashi, Publisher: Artech House Publishers, ISBN-13 : 978-1608070398
3. Identity & Access Management: A Systems Engineering Approach By Omondi Orondo, Kindle Edition

Supplementary Reading:

Web Resources:

1. Bishop, Matt, Elizabeth Sullivan, and Michelle Ruppel. 2019. Computer Security: Art and Science. Boston: Addison-Wesley. ISBN-13: 9780321712332

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Web links:

1. https://www.simplilearn.com/cyber-security/cissp-certification-training?source=lecture_pages#course-curriculum
2. https://www.simplilearn.com/identity-and-access-management-tutorial-video

MOOCs:

1. https://www.udemy.com/course/identity-access-management-learn-oauth-openidsaml-ldap/
2. https://www.udemy.com/course/identity-and-access-management-iam/

Pedagogy:

1. PowerPoint Presentation
2. Two Teacher Method
3. Videos
4. Flipped Classroom Activity
5. Expert lectures

Assessment Scheme:
Class Continuous Assessment (CCA) : 30 Marks

Assignments	Mid-Term Exam	Active Learning/ Case study
5 Marks	15 Marks	10 Marks

Laboratory Continuous Assessment (LCA): 30 Marks

Lab Assignment / Practical Performance	Oral
20 Marks	10 Marks

Term End Examination: 40 Marks

Syllabus: Theory

Module No.	Contents	Workload in Hrs. Theory
1	**Identity and Access Management Concepts** Introduction to IAM, Understanding Assets, Perimeter Security Management, Consumer IAM, Importance of Identity and Access Management in Security, Consequences of Lack in Identity Management, IAM Lifecycle. **Concepts:** Identity, Entitlement, Provisioning, De-provisioning. Identification Proofing, Fundamental Process of Identification, Authentication Reuse, RFID Tokens, Biometric Consideration,	09

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

	Authorization, Data Visibility, Access Control Principles, Accounting, Identification, Centralized Accounting. Identity and Access Management (IAM) Framework, IAM Principals: Principle of Least Privilege, Segregation of Duties, Identification Authentication, Authorization and Accountability (IAAA), Authentication Factors, Multi Factor Authentication, Controlling Physical and Logical Access to Assets	
2	**Access Management Models** **Access Control Model:** Types, Mandatory access control, comparing information flow in BLP and BIBA models, combining the BLP and BIBA models, Chinese wall problem. Discretionary access control and Access matrix model, definitions, Safety problem, The take grant protection model, Schematic protection model, SPM rules and operations, Role Based Access Control, Hierarchical Access Control, Mapping of a mandatory policy to RABC, Mapping discretionary control to RBAC, RBAC flow analysis, Separation of Duty in RBAC, RBAC consistency properties, Comparing Access Management Models, Privileged Access Management, Access Control Attacks.	09
3	**Organizational Processes, Governance, IAM Guidance and Standards** **Organizational Processes:** Introduction, Review and approval of Organizational Processes, Derived Credentials in Organizations, Self Service and Automation, De-provisioning. **Governance:** Introduction, Stakeholders, culture and Awareness, Centralized Vs Decentralized approaches, policy Vs Procedure. **IAM Guidance and Standards**: Understanding Guidance and Standards, Common Issues in Identity and Access Management, Federated Identity and Single Sign On (SSO), Federation Identity Management.	09
4	**Cloud Services and IAM Implementation** Introduction to Cloud Services, Cloud Service Model, Backend-as-a-Service-Firebase, Understanding Cloud Consideration, Password Options. Implementation of IAM, Multifactor Authentication Concepts and Implementations, Use cases and Functional Requirement, Interdependencies and Strategic Fit, Resource Implication	07
5	**Identity and Access Management Technologies** Technologies relating to IAM, Forms of Authentication- Kerberos, Active Directory and LDAP, Public Key Infrastructure, PKI approach to trust establishment, Open System Interconnected Model, Secure Sockets Layer and Transport Layer Security, Open Authorization, Components within XACML.	11

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

	Remote Authentication Dial-In User Service (RADIUS) Protocol, Terminal Access Controller Access Control System (TACACS and TACACS+), DIAMETER Protocol **Identity Federation Protocols:** Security Assertion Markup Language (SAML), OAuth, OPENID, Difference Between SAML, OpenID and OAuth Elements of trust paradigms in computing, Third party approach to identity trust, explicit third party authentication paradigm, Attribute certificates, Generalized web of trust models, Commercial Access Control Products and Tools, Current Issues with Identity and Access Management (IAM), IAM Case Studies (Retail/Banking Sector Identity and Access Management)	

Laboratory:

Assignment No.	Assignment Title	Workload in Hrs.
		Lab
1.	Installation of Windows Server system, Managing Windows Accounts and Organizational Units.	04
2.	Demonstration on i) Managing Identities in a Digital World. ii) Eliminating vulnerabilities in identification and authentication processes.	04
3.	Installation, Configuration and Managing Identity and access in Microsoft 365.	02
4.	Demonstration on ensuring strong authentication and configuring multifactor authentication	02
5.	Working with Active Directory Services and Extending on-premises Active Directory (AD) to Azure AD	02
6.	Implementing SSO in Azure for Office 365 and SaaS applications	02
7.	Authenticating with Amazon IAM roles	02
8.	Implementing Single Sign-On (SSO), Interoperating via open industry standards, federated logon and claims and Applying Kerberos identities in a domain.	04
9.	Demonstrating On-premises and cloud-based identity management	02
10.	Exploring identities in Kerberos tickets and AD attributes. Also Identifying identities in SQL databases	02
11.	Demystifying MIM 2016 ▪ Importing identities from Connected Data Source CDS into Connector Space CS ▪ Synchronizing identities into Metaverse MV ▪ Managing identities and rules with the SharePoint MIM Portal	04

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Dr. Vishwanath Karad
MIT WORLD PEACE UNIVERSITY PUNE
MIT-WPU

COURSE STRUCTURE

Course Code	**CET3026B**			
Course Category	**Professional Core**			
Course Title	**Artificial Intelligence and Machine Learning Techniques**			
Teaching Scheme and Credits Weekly load hrs	**Lecture**	**Tutorial**	**Laboratory**	**Credits**
	3 hr/wk	**--**	**2hr/wk**	**3 + 1 = 4**

Pre-requisites:

- Mathematics and statistics
- Programming Languages

Course Objectives:

1. **Knowledge:** (i) Understanding Artificial Intelligence (AI) principles and approaches.
   (ii) Learn basic concepts and techniques of Machine Learning (ML) and the need for Machine learning techniques for real world problem.
2. **Skills:** (i) Develop a basic understanding of the building blocks of AI as presented in of intelligent agents
   (ii) To provide understanding of various Machine learning algorithms and the way to evaluate the performance of ML algorithms
3. **Attitude:** (i) The objective of this course is provide an in depth knowledge of AI and ML

Course Outcomes:

After completion of this course students will be able to:

1. Apply difficult real-life problems in a state space representation to solve those using AI techniques like searching and game playing.
2. Formulate and solve given problem using Propositional and First order logic.
3. Apply machine learning techniques in the design of computer systems.
4. To differentiate between various categories of ML algorithms
5. Apply neural network learning for solving AI problems

Course Contents:

1. Overview of AI
2. Knowledge Representation
3. Reasoning and ML
4. Supervised learning
5. Neural Networks and Unsupervised learning

Laboratory Exercises:

1. Write a Program to Implement Breadth First Search / Depth First Search
2. Write a Program to Implement A* Algorithm for 8 puzzle problem
3. Study of Prolog programming language and Its function. Write Simple Facts for the statements using PROLOG

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Dr. Dinesh Seth
Dean

4. Write a program to implement a logistic regression for a given dataset, e. g. titanic dataset / pima Indian diabetes database
5. Write a program to implement SVM classifier, compare with decision tree algorithm
6. Write a program to implement Naïve Bayes classifier / neural network classifier
7. Write a program to implement anyone clustering algorithm such as k-means clustering algorithm on a given data
8. Mini Project

Learning Resources:

Text Books:

1. Elaine Rich and Knight, Artificial Intelligence, McGraw-Hill Publications
2. Artificial Intelligence: A modern Approach, Russell and Norvig, Prentice Hall
3. E. Alpaydin, Introduction to Machine Learning, PHI, 2004.
4. Stephen Marsland, Machine Learning an Algorithmic Perspective 2nd Edition, 2015, Taylor & Francis Group, LLC
5. Tom M Mitchell, Machine Learning, 1st Edition, McGraw Hill Education, 2017

Reference Books:

1. Patterson, Introduction To Artificial Intelligence & Expert Systems, PHI
2. Weiss. G, Multi Agent systems- a modern approach to Distributed Artificial intelligence, MITPress.
3. Shaishalev-shwartz, Shai Ben-David: Understanding Machine Learning from Theory to algorithms, Cambridge University Press, ISBN-978-1-107-51282-5, 2014.

Supplementary Reading:

1. Power Point Slides
2. Question Bank

Web Resources:

1. Machine Learning - https://www.w3schools.com/ai/
2. AI - https://www.javatpoint.com/artificial-intelligence-ai

Web links:

1. https://onlinecourses.nptel.ac.in/
2. https://www.edx.org/
3. https://in.coursera.org/
4. https://www.udemy.com/

MOOCs:

1. AI for Everyone – https://www.learndatasci.com/best-artificial-intelligence-ai-courses/
2. Machine Learning - https://www.coursera.org/specializations/machine-learning

Pedagogy:

1. Power Point Slides
2. Videos
3. Expert Lectures

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Assessment Scheme:

Class Continuous Assessment (CCA): 30 Marks

Mid Term	Component 1 (Active Learning)	Component 2 (Theory Assignment)
15 Marks	10 Marks	5 Marks

Lab Continuous Assessment (LCA): 30 Marks

Practical Performance	Mini Project	End Term Oral Performance
10 Marks	10 Marks	10 Marks

Term End Examination: 40 Marks

Syllabus: Theory

Module No.	Contents	Workload in Hrs
		Theory
1	**Overview of AI** **AI Fundamentals:** Defining Artificial Intelligence, Defining AI techniques, AI Applications. State Space Search and Heuristic Search Techniques: Defining problems as State Space search, Production systems and characteristics, Local search: Hill Climbing, Breadth first and depth first search, Informed search such as best-first search, A* algorithm, introduction to game playing, minimax algorithm **Knowledge Representation Issues:** Representations and Mappings, Approaches to knowledge representation	9
2	**Knowledge Representation** **Using Predicate Logic and Representing Knowledge as Rules:** Representing simple facts in logic, Computable functions and predicates, Procedural vs. Declarative knowledge, Logic Programming, forward vs. backward reasoning **Symbolic Reasoning under Uncertainty:** Non-monotonic Reasoning, Logics for non- monotonic reasoning	9
3	**Reasoning and ML** **Reasoning:** Probability and Bayes Theorem, Certainty factors, Probabilistic Graphical Models, Bayesian Networks, Markov Networks, Fuzzy Logic. **Introduction to Machine Learning:** Idea of Machines learning from data, Classification of problem – Regression and Classification, Types of machine learning, Supervised and Unsupervised learning.	9

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

4	**Supervised learning** **Supervised learning:** Linear Regression: Model representation for single variable, Single variable Cost Function, Gradient Decent for Linear Regression, Multivariable model representation, Multivariable cost function, Gradient Decent in practice, Normal Equation and non-invertibility **Logistic Regression:** Classification, Hypothesis Representation, Decision Boundary, Cost function, Advanced Optimization, Multi-classification (One vs. All), Problem of Over fitting, Regularization **Classification Problems:** Support Vector Machines: Optimization Objective, Large Margin Classifiers, Kernels, SVM practical considerations, Decision Tree classifier	9
5	**Neural Networks and Unsupervised learning** **Neural Networks**: Non-linear Hypothesis, Biological Neurons, Model representation, Intuition for Neural Networks, Multiclass classification, Cost Function, Back Propagation Algorithm, Back Propagation Intuition, Weights initialization, Neural Network Training **Unsupervised learning:** Unsupervised learning introduction, Types of clustering algorithms, k-Means clustering Algorithm, Optimization objective, Random Initialization, Choosing number of clusters.	9

Lab Assignments

Sr No.	Contents	Workload in Hrs
		Lab
1	Write a Program to Implement Breadth First Search / Depth First Search	2
2	Write a Program to Implement A* Algorithm for 8 puzzle problem	4
3	Study of Prolog programming language and Its function. Write Simple Facts for the statements using PROLOG	2
4	Write a program to implement a logistic regression for a given dataset, e. g. titanic dataset / pima Indian diabetes database	2
5	Write a program to implement SVM classifier, compare with decision tree algorithm	4
6	Write a program to implement Naïve Bayes classifier / neural network classifier	4
7	Write a program to implement anyone clustering algorithm such as k-means clustering algorithm on a given data	4
8	Mini Project	4

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Dr. Dinesh Seth
Dean

Dr. Vishwanath Karad
MIT WORLD PEACE UNIVERSITY PUNE

COURSE STRUCTURE

Course Code	**CET4032B**			
Course Category	**Program Core**			
Course Title	**Security Management and Cyber Laws**			
Teaching Scheme and Credits	**Lecture**	**Tutorial**	**Laboratory**	**Credits**
Weekly load hrs.	**03 hrs/ week**	**01 hr /week**	**-**	**03+01=04**

Pre-requisites:

- Software Engineering and Testing
- Information and Cybersecurity

Course Objectives:

1. Knowledge (i) To understand the basics of security management.
(ii) To introduce security management models.

2. Skills (i) To understand the importance of security planning and contingencies.
(ii) To learn about the legal frameworks.

3. Attitude (i) To explore critical understanding of cyber law for Cyber-crimes.

Course Outcomes

After completion of this course students will be able to-

1. Describe and identify security policy framework, legal and moral implication and best practices in security management
2. Describe the need for and development of information security policies, and identify guidelines and models for writing policies
3. Design detailed enterprise wide security auditing plans and processes
4. Demonstrate a critical understanding of the Cyber law with respect to Indian IT/Act 2008

Course Contents:

- Introduction to Security Management
- Planning for Security and Contingencies
- Implementing Security Management
- Legal Framework
- Cyber law for Cyber Crimes

Learning Resources:

Here are some text and reference books that will be recommended for the course.

Text Books

1. Principles of Information Security, Michael E. Whitman, Herbert J. Mattord
2. Cyber Security, understanding cybercrimes, computer forensics and legal perspectives by Nina Godbole, and Sunit Belapure, WILEY Publication (2011), ISBN: 9788126521791.

MIT-WPU
Approved by
Academic Council
Date 08 JUN 2023

Dr. Dinesh Seth
Dean

Reference Books

1. Sennewald, C., and Baillie, C. (2011). Effective Security Management. Elsevier Publication.
2. Handbook of Information Security Management, Micki Krause, Harold F. Tipton, Isc2 Press.
3. Information Security Policies, Procedures, and Standards - A Practitioner's Reference by Douglas Landoll. CRC Press, 2016 ISBN: 1482-24589-2
4. Cyber Crime Manual by Bibhas Chatterjee, Lawman Publication
5. Jonthan Rosenoer, Cyber Law, Springer, New York, (1997)

Supplementary Reading

1. Power Point Slides
2. Case Study
3. Practice Assignments

Web Resources

1. http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
2. http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

Pedagogy:

- PPTs
- Practical Demos
- Videos
- Expert lectures
- Workshop/Audit reports
- Co Teacher Scheme

Assessment Scheme

Class Continuous Assessment: 60 Marks

Midterm Exam	Component 1	Component 2	Component 3
15 Marks	15 Marks	15 Marks	15 Marks

Lab Continuous Assessment (LCA) : NA

Term End Examination: 40 marks

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Dr. Dinesh Seth
Dean

Syllabus:

Module No.	Contents	Workload in Hrs Theory
1	**Introduction to Security Management** Basics of Security, Principles of Information Security Management, Need for Security: Threats, Attacks. Planning for Security, The role of Planning, Information Security Governance. Information Security Policy, Standards, and Practices, Planning for Information Security Implementation, Types of Information Security Policy, Guidelines for Effective Policy, Information Security Roles and Titles. Security Education, Training, and Awareness Program.	**09**
2	**Security Management Model** Blueprints, Framework and Security Models, Access Control Models, Security Architecture Models, Security Management Models- ISO 270000 Series, NIST Security Models, SP 800-53A, COBIT, COSO, IT Infrastructure Library, Information Security Governance Framework.	**09**
3	**Implementing Security Management** Information Security Project Management, Benchmarking, Performance Measure in Information Security Management-InfoSec Performance Measure: Management, Metrics, Building, Collecting, Implementing, Reporting, Emerging Trends in Certification and Accreditation - SP 800-37, SP 800-53, Security Management Practices and Auditing	**09**
4	**Legal Framework and Cyber Law** Introduction, Cybercrime and the Legal Landscape around the World, The Indian IT Act, Challenges to Indian Law and Cybercrime Scenario in India, Digital Signatures and the Indian IT Act, Amendments to the Indian IT Act.	**09**
5	**Cyber law for Cybercrime** Need for Cyber Law, Cyber Jurisprudence at International and Indian Level, Cybercrime and Punishment, Cyber Crimes & Legal Framework Cyber Crimes against Individuals, Institution and State, Hacking, Digital Forgery, Case studies.	**09**

MIT-WPU
Approved by
Academic Council
Date 08 JUN 2023

Dr. Dinesh Seth
Dean

COURSE STRUCTURE

Course Code	**CET4033B**			
Course Category	**Professional Core**			
Course Title	**Digital Forensics and Investigation**			
Total Teaching Hrs and Credits	**Lectures**	**Tutorial**	**Laboratory**	**Credits**
	02 hrs/week	**--**	**02 hrs/week**	**2+1=03**

Pre-requisites

- Computer Networks, Information Security

Course Objectives:

1. To explore the investigative aspect of digital crimes
2. To understand computer forensics
3. To learn tools used in digital forensics
4. To learn basic programming for digital forensics

Course Outcomes:

On completion of course, students should be able to

1. Develop awareness of computer forensics
2. Conduct effective investigation of digital crimes
3. Analyze and use digital forensics tools for efficient investigation
4. Employ digital forensics applications in real world

Course Contents:

1. Introduction to Digital Forensics
2. Evidence Collection
3. Windows and Linux Forensics
4. Security Tools
5. Case Study and Scenarios

Laboratory Exercises:

1. Explore various computer forensic application programs for recovering deleted files and or deleted partitions and demonstrate any one such tool.
2. Write a program in C++ /Python to analyze an email header.
3. Write a program for identifying tampering in either image or voice data. Use big data as input.
4. Install a suitable Digital Forensics framework (such as Encase) and perform investigation. Generate the various reports and analyze the same.
5. Write a Java/Python program to monitor and analyze Network Forensics, also perform investigation of various logs
6. Perform installation and employ any Android Mobile Forensics Open Source Tools for real time investigation of mobile forensics
7. Develop a C++/Java program for Log Capturing using a wireless router. Perform suitable event correlation and analysis of network traffic.
8. Demonstrate Forensics Case Investigation using Autopsy

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Learning Resources:

Text Books:

1. Digital Evidence & Computer Crime, Eoghan Casey Bs Ma Ac, Elsevier-Academic Press, Third Edition, ISBN 13: 978-0123742681, ISBN 10 : 0123742684
2. Computer Forensics Jump Start- Michel G. Solomen, Diane Banet and Neil Broom

Reference Books:

1. Hacking Exposed- Computer Forensics Chris Davis, Aaron Phillipp and Davidcowen. Ma-Graw Hill
2. Forensics and Investigative accounting- D Larry Crumbley, Laster E. Heitger and G. Stevenson smith.

Supplementary Reading:

Code Hacking- Richard Conway and Julian Cordingley

Web Resources:

https://www.forensicfocus.com/
https://www.youtube.com/watch?v=F7mH5vz1qEI&featur=yotu.be

Web links:

http://www.cca.gov.in/
https://www.verisign.com/
https://meity.gov.in/content/information-technology-act-2000

MOOCs:

https://swayam.gov.in/NPTEL
https://nptel.ac.in/noc/
https://www.edx.org/course/computer-forensics

Pedagogy:

1. Power Point Presentation
2. Video Lectures
3. Flipped Classroom Activity

Assessment Scheme:

Class Continuous Assessment: 30 Marks

Assignments	Mid Term Exam	Active learning	Total
5 Marks	15 Marks	10 Marks	30 Marks

Laboratory Continuous Assessment: 30 Marks

Practical	Problem based Learning/ Tool Demo	Oral	Total
10 Marks	10 Marks	10 Marks	30 Marks

Term End Examination: 40 Marks

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Dr. Dinesh Seth
Dean

Syllabus: Theory

Module No.	Contents	Workload in Hrs Theory
1	**Introduction Digital Forensics** Introduction to Digital Forensics, Locard's Principle of Exchange in Digital Forensics, Branches of Digital Forensics, Principles of Digital Forensics, Phases of digital/computer forensics investigation, Identification of digital evidences, necessary documentations such as Chain of Custody, pre-acquisition forms etc., Digital evidence handling at crime scene as per standards, Collection/Acquisition and preservation of digital evidences, Processing & analysis, Compilation of findings & Reporting. Code Hacking- Input Validation, Buffer Overflow Attacks, SQL Injection, Cross Site Scripting , Ethical hacking of operating Systems, Ethical hacking of web, email and mobile Phones	08
2	**Evidence Collection** Challenges in dealing with Digital Evidence Defining levels of certainty in Digital Evidence, Computer Forensics: Incident Response Secrets and solutions, Investigations – Covert and remote operations, Search and seizure of digital evidence, Data Acquisition and disk imaging, Special Forensics Scenarios : Email Forensics Investigation, Data storage Forensics, Forensic Investigation of mobile devices, Forensic investigation of Wi-Fi Environment	08
3	**Windows and Linux Forensics** Understanding registry concept in various operating systems, Log analysis with respect to standalone machine and server which includes system logs, kernel logs, event logs etc. Windows Forensics: Locate and Gather Evidence, File Slack and its Investigations, Interpret the Windows Registry, Internet Traces, System State Backups, File System Description in Linux, Linux Directories, The Challenges in Disk Forensics with Linux, Linux Forensics Tool: SMART for Linux Forensics	08
4	**Security Tools** Open Source Tools (Forensics tools Suites) TCT (The Coroners Toolkit), TSK (The Sleuth Kit), FTK (Forensics Tool Kit), EnCaseMaresware. Security Software: Antivirus, Email Security, Identify and Access Management, Incidence response policies, Incidence reporting Forensics & Intrusion Detection, and Prevention. **Case Study and Scenarios** IP Thefts, Corporate Frauds, Digital Frauds, Cyber Crimes, Cyber Porn, Cyber Stalking, Consumer and credit Card Fraud, Online and Digital Fraud-Phishing Attacks, Spare Attack and other Incident.Forensic analysis of Multimedia Files, CCTV Footage analysis, Different Steganalysis tools and techniques	08

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Laboratory:

Module No.	Contents	Workload in Hrs
		Lab
1.	Write a program in C++ /Python to analyse an email header.	04
2.	Perform installation and employ any Android Mobile Forensics Open Source Tools for real time investigation of mobile forensics	02
3.	Write a Java/Python program to monitor and analyse Network Forensics, also perform investigation of various logs.	02
4.	Write a program for identifying tampering in either image or voice data. Use big data as input.	02
5.	Develop a C++/Java program for Log Capturing using a wireless router. Perform suitable event correlation and analysis of network traffic.	02
6.	Explore various computer forensic application programs for recovering deleted files and or deleted partitions and demonstrate any one such tool.	02
7.	Install a suitable Digital Forensics framework (such as Encase) and perform investigation. Generate the various reports and analyse the same.	04
8.	Demonstrate Forensics Case Investigation using Autopsy	04

MIT-WPU
Approved by
Academic Council

Date...../...../.....

Dr. Dinesh Seth
Dean

Dr. Vishwanath Karad
MIT-WPU MIT WORLD PEACE UNIVERSITY PUNE

COURSE STRUCTURE

Course Code	CET4034B			
Course Category	Program Core			
Course Title	Cloud Infrastructure and Security			
Teaching Scheme and Credits	Lectures	Tutorial	Laboratory	Credits
Weekly load hrs	2hr/wk	--	02 hr/wk	2 + 1 = 3

Pre-requisites:

- Mathematics and Programming

1) **Knowledge** **(i)** To study basic cloud computing concepts and its operational environment.
2) **Skills** **(i)** To acquire skills of using various Virtualization Techniques and Platforms
   (ii) To Understand challenges in Cloud Computing
3) **Attitude** **(i)** To select and use cloud computing platform

Course Outcomes:

After completion of this course students will be able to:

1. Set-up a cloud environment
2. Deploy web services efficiently on a cloud platform
3. Manage Cloud services efficiently and effectively
4. Design, deploy & address the cloud security aspects

Course Contents:

Course Contents:

1. Introduction To cloud Computing
2. Understanding Virtualization
3. Amazon Web Service
4. Security in cloud computing

Lab Assignments :

1. Virtualization
2. PaaS
3. IaaS : AWS EC2
4. IaaS : AWS S3
5. Docker

Learning Resources:

Text Books:

1. Rajkumar Buyya, Christian Vecchiola, S. Thamarai Selvi, "Mastering Cloud Computing", Tata McGraw Hill, ISBN-13: 978-1-25-02995-0
2. Tim Mather, Subra K, Shahid L, Cloud Security and Privacy, OReilly, ISBN-13 978-81-8404-815-5
3. Rajkumar Buyya, James Broberg, Andrzej Goscinski, "Cloud computing Principles and Paradigms", Wiley Publication.
4. Barrie Sosinsky, "Cloud Computing", Wiley India, ISBN: 978-0-470-90356-8

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

5. Kailash Jayaswal, "Cloud computing", Black Book, Dreamtech Press
6. Thomas Erl, Zaigham Mahmood and Ricardo Puttini, "Cloud Computing: Concepts, Technology and Architecture", Pearson, 1st Edition.

Reference Books:

1. Introduction to the Theory of Computation, Michael Sipser.
2. Introduction to Languages and the Theory of Computation, John Martin.
3. Computers and Intractability: A Guide to the Theory of NP Completeness, M. R. Garey and D. S. Johnson

Supplementary Reading:

1. Dr. Kumar Saurabh, "Cloud Computing", Wiley Publication

Web Resources:

E-books:

1.https://www.ibm.com/cloud-computing/files/cloud-for-dummies.pdf

Web-Links:

1. https://docs.aws.amazon.com/
2. https://docs.microsoft.com/en-us/azure/

MOOCs (Coursera)

1. https://www.coursera.org/learn/gcp-fundamentals
2. https://nptel.ac.in/courses/106105167/

Pedagogy:

1. Team teaching
2. Audio- video techniques
3. Tutorials and class tests

Assessment Scheme:

Class Continuous Assessment (CCA): 30 marks

Mid Term	Component 1 (Active Learning)	Component 2
15 Marks	10 Marks	5 Marks

Laboratory Continuous Assessment (LCA): 30 marks

Practical Performance	Active Learning/Mini Project/ Additional Implementation/On paper Design	End term Practical/Oral Examination
10 Marks	10 Marks	10 Marks

Term End Examination: 40 Marks

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Syllabus: Theory

Module No.	Contents	Workload in Hrs.
1.	**Introduction To cloud Computing** Introduction, Roots of Cloud Computing: From mainframe to Cloud, Benefits of Cloud Computing SOA, Web services, Role of Networks in Cloud Computing: Cloud types and service models, Primary Cloud Service models, Cloud Services brokerage, Primary cloud deployment models, cloud computing reference model, The greenfield and brownfield deployment options.	8
2.	**Understanding Virtualization** Virtualization, Concept of Hypervisor, Types of Hypervisor, Taxonomy of Virtualization, Virtualization and machine reference model, Hardware virtualization techniques, Pros and Cons of Virtualization, Live migration, Technology examples: Xen, KVM, VMware, Microsoft Hyper-V.	7
3.	**Amazon Web Service** Services offered by Amazon Hands-on Amazon, EC2 - Configuring a server, Virtual Amazon Cloud, AWS Storage and Content Delivery Identify key AWS storage options Describe Amazon EBS Creating an Elastic Block Store Volume. Create an Amazon S3 bucket and manage associated objects. AWS Load Balancing Service Introduction Elastic Load Balancer Creating and Verifying Elastic Load Balancer	8
4.	**Security in cloud computing** Introduction, Global Risk and Compliance aspects in cloud environments and key security terminologies, Digital identity and access management, Content level security **Future of Cloud computing:** Docker, serverless lambda, MicroServices, Cloud Forensics	7

Syllabus: Practical

Assignment No	Title of the Assignment	Workload in Hrs.
1	Install VM-Ware Workstation on a windows platform and deploying an Ubuntu server VM as per requirement.	4
2	Write a web service using java or python. Deploy the service using PaaS tools such as cloud Cloud Foundry/ GoogleAppEngine/OpenShift.	4
3	Create an account on AWS. Deploy a website for admission portal on the EC2 Service. Configure the Traffic rules of the Server for a specific need. Creation of Application Load Balancer	4
4	Write a program to Manage and monitor S3 operations to a specific Account using BOTO3 or equivalent libraries.	4
5	Install Docker on Windows/Ubuntu operating system	4
6	Miniproject	10

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

COURSE STRUCTURE

Course Code	**CET2008B**			
Course Category	**Professional Core**			
Course Title	**Theory of Computation**			
Teaching Scheme and Credits	**Lectures**	**Tutorial**	**Laboratory**	**Credits**
Weekly load hrs	**3hr/wk.**	**--**	**--**	**3**

Pre-requisites:

- Data Structures
- Discrete Mathematics

Course Objectives:

1.**Knowledge:**

i. To learn Automata theory, Regular Expression from the perspective of formal languages
ii. To learn Context Free Grammar, Pushdown Automata, Turing Machine and Complexity Theory

2. Skills:

i. To aquent with various applications of Automata Theory
ii. To realize Industry relevance of Automata Theory

3. Attitude:

i. To apply automata theory concepts in design and c implementation of Compilers.
ii. To apply automata theory concepts in various domains.

Course Outcomes:

After completion of this course students will be able to:

1. To construct Finite Automata to solve problems in computing
2. To build regular expressions and understand regular language
3. To construct context-free grammar and Push Down Automata
4. To design computational models and classify the problems of decidability

Course Contents:

1. Introduction to Automata
2. Regular Expression (RE)
3. Context Free Grammars (CFG) and Pushdown Automata
4. Turing Machine
5. Basic Introduction to Complexity

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
Date 08 JUN 2023

Learning Resources:

Text Books:

1. Vivek Kulkarni, Theory of Computation, Oxford University Press, ISBN-13: 978-0-19-808458-7
2. K.L.P Mishra, N. Chandrasekaran, Theory of Computer Science (Automata, Languages and Computation), Prentice Hall India, 2nd Edition.

Reference Books:

1. Introduction to the Theory of Computation, Michael Sipser.
2. Introduction to Languages and the Theory of Computation, John Martin.
3. Computers and Intractability: A Guide to the Theory of NP Completeness, M. R. Garey and D. S. Johnson

Supplementary Reading:

1. Hopcroft Ullman, Introduction to Automata Theory, Languages and Computations,

Pearson Education Asia, 2nd Edition, ISBN: 9788131720479

Web Resources:

1. https://www.tutorialspoint.com/automata_theory/index.htm

MOOCs:

1. https://www.udemy.com/course/formal-languages-and-automata-theory-e
2. https://nptel.ac.in/courses/106104148

Pedagogy:

1. White Board/Smart Board
2. PowerPoint Presentations
3. Blended Learning (Combination of online and / on campus classes)
4. Group Activity

Assessment Scheme:

Class Continuous Assessment (CCA): 60 Marks

Mid Term	Component 1 (Active Learning)	Component 2	Component 3
15 Marks	15 Marks	15 Marks	15 Marks

Term End Examination: 40 Marks

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Dr. Dinesh Seth
Dean

Syllabus: Theory

Module No.	Contents	Workload in Hrs. Theory
1	**Introduction to Automata:** Computability and Complexity theory: Concepts of Automata Theory: Alphabet, languages and grammars, productions and derivation, Introduction to Finite Automata, Simplified notation: State transition graph, Transition table, Acceptance of a string, Acceptance of a Language, Deterministic finite Automata (DFA)-Formal Definition, Non Deterministic Finite Automata (NFA)-Formal Definition, Non-Deterministic Finite Automata (NFA) with epsilon transition, Equivalence of NFA and DFA, Conversion from NFA to DFA, Conversion from NFA with epsilon transition to DFA, Minimization of finite automata. Finite Automata with output: Moore and Mealy Machine, Moore to Mealy conversion, Mealy to Moore conversion	10
2	**Regular Expression (RE):** Definition, Operators of regular expression and their precedence, Algebraic laws for Regular expressions, Kleene's Theorem: Equivalence Regular expressions and DFAs, Closure properties of Regular Languages (union, intersection, complementation, concatenation, and Kleene closure), Applications of Regular expressions. DFA to RE, Using Arden's Theorem, Pumping Lemma for regular languages	9
3	**Context Free Grammars (CFG) and Pushdown Automata:** Formal definition of Grammar, Chomsky Hierarchy, CFG: Formal definition of CFG, Derivations, Parse Tree, Ambiguity in grammars and languages, Language Specification using CFG, Normal Forms: Chomsky Normal Form and Greibach Normal Form. Closure properties of CFL. Applications of CFG. Pushdown Automata: Description and definition, Language of PDA, Acceptance of PDA by final State and Empty Stack, Designing PDA, Equivalence of Pushdown Automata and CFG, Deterministic Pushdown Automata, Nondeterministic Pushdown Automata, Intersection of CFLs and Regular language, Introduction to Context-sensitive languages and Context-sensitive grammars (CSG)	10
4	**Turing Machine:** Formal definition of a Turing Machine, Church-Turing Thesis and intuitive notion of Algorithm, Instantaneous Description, Recursive Languages and Recursively Enumerable Languages, Design of Turing Machines, Robustness of Turing Machine model and equivalence with various variants: Universal Turing Machine, Nondeterministic Turing machines, multi-tape TM, Designing TM	8
5	**Basic Introduction to Complexity:** Concept of Decidability, Un-decidability, Undecidability of Halting problem. Examples of undecidable problems: Post Correspondence Problem, Introductory ideas on Time complexity of deterministic and nondeterministic Turing machines, P and NP, Example of NP-Complete and NP Hard problems.	8

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Dr. Vishwanath Karad
MIT WORLD PEACE UNIVERSITY PUNE
MIT-WPU

COURSE STRUCTURE

Course Code	**CET4010B**			
Course Category	**Professional Core (PC)**			
Course Title	**Vulnerability Identification and Penetration Testing**			
Teaching Scheme and Credits	**Lecture**	**Tutorial**	**Laboratory**	**Credits**
Weekly load hrs	**3**	**-**	**2**	**3+0+1=4**

Pre-requisites:

- Network Security

Course Objectives:

1. **Knowledge:**
   (i) Study the importance and benefits of Vulnerability Identification and Penetration Testing
   (ii) Learn ethical guidelines and industry best practices for performing Penetration Testing assessments
2. **Skills:**
   (i) Demonstrate the knowledge to perform Vulnerability Identification and Penetration Testing
3. **Attitude:**
   (i) Identify breaches/ Vulnerability found in a network using Penetration Testing

Course Outcomes:

After completion of the course the students will be able to :-

1. Understand how to exploit a program and different types of software exploitation techniques
2. Understand the exploit development process
3. Search for vulnerabilities in closed-source applications
4. Analyze and apply different VAPT tools and generate report

Course Contents:

1. Vulnerability Identification
2. Penetration Testing-Principles and Practices
3. Penetration Testing
4. VIPT Audit and uses cases

Learning Resources:

Text Books:

1. The Art of Network Penetration Testing by Royce Devis, copyright Manning Publications-2020.
2. Penetration Testing: A Hands-On Introduction to Hacking 1st Edition by Georgia Weidman, No-starch Press, ISBN-13: 978-1593275648

Reference Books:

1. Advanced Infrastructure Penetration Testing by Chiheb Chebbi, Packt Publishing Bermingham – Mumbai, 2018.
2. The basic of Hacking and Penetration testing, second edition on ethical hacking and penetration by Patrick Engebretson
3. Hack I.T. - Security Through Penetration Testing, T. J. Klevinsky, Scott Laliberte and Ajay Gupta, Addison-Wesley, ISBN: 0-201-71956-8

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

4. Metasploit: The Penetration Tester's Guide, David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni
5. Professional Penetration Testing: Creating and Operating a Formal Hacking Lab, Thomas Wilhelm

MOOCs:

https://swayam.gov.in/nd1_noc20_ma24/preview

Pedagogy:

- Power Point Presentation
- Two Teacher Method
- Video Lectures
- Flipped Classroom Activity

Assessment Scheme:

Class Continuous Assessment (CCA): 30 marks

Mid Term	Component 1 (Active Learning)	Component 2
15 Marks	10 Marks	5 Marks

Laboratory Continuous Assessment (LCA): 30 marks

Practical Performance	Active Learning/Mini Project/ Additional Implementation/On paper Design	End term Practical/Oral Examination
10 Marks	10 Marks	10 Marks

Term End Examination: 40 Marks

Theory Syllabus:

Module No.	Contents	Workload in Hrs
1	**Penetration Testing-Principles and Practices** Importance and benefits of Penetration Testing assessments. Penetration testing-Principles and concepts, PT work flows and examples, blind tests, Function of malware and destructive viruses. Ethical hacking techniques, Ethical guidelines and industry best practices for performing Penetration Testing assessments.	09
2	**Vulnerability Identification** Introduction to Metasploit: Metasploit framework, Metasploit Console, Payloads Using Nmap to sweep IP ranges for live hosts, Performance tuning Nmap scans. Discovering hosts using commonly known ports. Understanding security posture, cybersecurity issues. Gathering Information about target computer systems – Foot printing and	09

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

	Investigation. Scanning computers in the Networks. Network infrastructure vulnerabilities. Enumeration- Listing the systems/users and connecting them. Identifying Vulnerabilities associated with systems. Ethical hacking-penetrate into the security to locate vulnerabilities.	
3	**Penetration Testing** Exploring Ethical Hacking, Malware Threats and their Counter measures. Monitoring and Capturing Data Packets using Sniffing. Restricting the System Access – DoS Attack, Gather Confidential Information – Social Engineering. Vulnerability Issues: Operating System Vulnerabilities; Application Vulnerabilities; Vulnerability assessment for natural disaster, technological hazards and terrorist threats; implications for emergency response, vulnerability of critical infrastructures	09
4	**VIPT Audit and Uses cases** Discovering patching vulnerabilities, Discovering web server vulnerabilities. Synthetic transactions, interface testing and fuzzing, SDLC phases and security mandates. Perform Penetration Testing assessments, detect and respond to network breaches found in Penetration Testing assessments. Preparation of a Penetration Test report, Auditing the Systems, Analysis and Reporting. Case Studies of recent vulnerabilities and attacks.	09
5	**Attacks** Exploitation-exploiting default credentials, exploiting buffer overflow in third party software, Password attacks-online password attacks, offline password attacks, Client side exploitation- bypassing filters with metasploit payload, Client side attacks, bypassing antivirus applications, Social Engineering- spear phishing attacks	09

Laboratory:

Vulnerability Identification and Penetration Testing

The course faculty should frame the suitable assignments/problem statements based on the concern theory subject. Concerned faculty member may add/modify the assignment list as per the need of the course.

There will be continuous evaluation of these assignments during the Trimester. Student has to submit a Journal/report consisting of suitable write up in the prescribed format. Softcopy of journal/report and code is to be maintained at department/institute in digital repository. Faculty advisor/ laboratory instructor suggested language/platform/framework is to be used for completing assignments/mini-project.

Guidelines for Term Work Assessment

Continuous assessment of laboratory work is done based on performance of student. Each assignment/ mini project assessment to be done based on parameters with appropriate weightage. Faculty should do the overall assessment as well as mini project assessment be based on the suggested parameters.

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Laboratory :

Module No.	Contents
1	Generate Brute-force password-guessing attacks. Use Password cracking tools – Air-crack-ng
2	Find sweep IP ranges for live hosts and Performance tuning using Nmap scans
3	Obtain network services from an attacker's perspective using Nmap
4	Discover Network service to Organize and Sort through Nmap scan output
5	Creating protocol-specific target lists for vulnerability discovery
6	Obtain threats associated with Web Servers & Applications. i.e. Session Hijacking
7	Implementation to gather information from any PC's connected to the LAN using whois, port scanners, network scanning, Angry IP scanners etc.
8	Implementation of IT Audit, malware analysis and Vulnerability assessment and generate the report.

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Dr. Dinesh Seth
Dean

Dr. Vishwanath Karad
MIT WORLD PEACE UNIVERSITY | PUNE
TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

COURSE STRUCTURE

Course Code	CET4006B			
Course Category	Professional Elective II			
Course Title	Data Privacy			
Teaching Scheme and Credits	Lecture	Tutorial	Laboratory	Credits
Weekly load hrs.	03 hr/wk	--	02 hr/wk	3+1 = 04

Pre-requisites:

- Information Security

Course Objectives:

1.Knowledge

i. Understand the mathematics required for cryptographic algorithms
ii. Describe data privacy preserving techniques

2.Skills

i. Implement cryptographic algorithms
ii. Implement data privacy preserving techniques

3.Attitude

i. Demonstrate the use of privacy preserving techniques in real life examples

Course Outcomes:

After completion of the course the students will be able to: -

1. Remembering: To recognize the importance of data privacy in real life
2. Understanding: To explain the mathematics required for cryptographic algorithms
3. Applying: To implement different privacy preserving techniques
4. Creating: To create privacy preserving application

Course Contents:

1. **Introduction to Data Privacy -** Data privacy and its importance, protecting sensitive data, privacy and anonymity, Use cases: Need for sharing data – Data Mining and analysis, Software application testing, business operations, Nature of data – multidimensional, transactional, longitudinal, graph, time series, Methods of protecting data – Cryptography, Anonymization, Tokenization
2. **Mathematics for Cryptography -** Mathematics for Asymmetric Keypair Cryptography, Rings, Groups, Cyclic Groups, RSA, ElGamal, Pailliers, Elliptic Curve, totient functions, Euclidean and extended Euclidean algorithm, Euler's theorem, Fermat's Theorem, Multiplicative Inverses
3. **Internet Cryptography -** HTTPS and Perfect Forward Secrecy, Signal Encryption Protocol. Hash Functions – MD family, SHA family, Hash Chains, Merkle Tree Entity

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

08 JUN 2023
Date...../...../.....

Syllabus: Theory

Module No	Content	Workload in Hrs. Theory
	Introduction To Data Privacy	

4	**Privacy Frameworks** Categories of Laws and Privacy compliances, Contracting and Procurement, Cyber Laws in India, Indian Data Privacy Law draft, GDPR Privacy standard, GDPR Principles, Right of data subjects, Controllers, Transfer of data regulations, Organization, Role of officers, Liability, NIST Cybersecurity framework - Data privacy	09
5	**Homomorphic Encryption** Homomorphic Encryption using Lattice Cryptography: CKKS, BFV. Homomorphic Encryption using Number Theory, Fundamentals of Differential Privacy System, Oblivious Transfer System and Protocol: Two-party and Multiparty settings.	09

Laboratory:

Sr. No.	List of Assignments	Workload in Hrs.
		Lab
1.	Implement and Simulate Key Exchange between two entities using Diffie–Hellman Key Exchange algorithm and protocol.	04
2.	Implement a client and a server on two different computers. Perform the communication between these two entities by using RSA (for key exchange) and AES 256 cryptosystem (for encryption)	04
3.	Implement a Random Number Generator and test its randomness using NIST Statistical test suite.	02
4.	Implement a Prime Number Generator.	02
5.	Implement Toy AES algorithm using any language of your choice	04
6.	Implement Toy RSA algorithm using any language of your choice.	02
7.	Download and Configure Java Kerberos System	02
8.	Implement Merklee Tree and using it for file integrity checks.	04
9.	Implement Differential Privacy	02
10.	Mini-Project: (Students can select any one topic from the following) 1. Privacy-Preserving Online Notes. 2. Privacy-Preserving DB for storing and retrieval of Patient Databases. 3. Privacy-Preserving DB for storing and retrieval for Travel data. 4. Privacy-Preserving Calendar Application. 5. Privacy-Preserving DB for storing and retrieval of financial data.	04

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
Date 08 JUN 2023

Dr. Vishwanath Karad
MIT WORLD PEACE UNIVERSITY | PUNE

MIT-WPU

COURSE STRUCTURE

Course Code	CET4036B			
Course Category	Professional Elective			
Course Title	Data Science for Cybersecurity and Forensics			
Total Teaching Hrs. and Credits	Lectures	Tutorial	Laboratory	Credits
	3	-	2	3+0+1=4

Pre-requisites

- Mathematics Linear Algebra
- Basic Programming

Course Objectives:

1. To study the core aspects of data and data based models
2. To learn statistical analysis methods and ways of data visualization
3. To learn how to manage different types of data in the case of cyber security
4. To be able to apply data science concepts and methodsearn the various data pre-processing methods used in python programming.
5. Learn through real word problems in cyber security and forensics.

Course Outcomes:

On completion of course, students should be able to

1. Develop the ability to build and assess data-based models.
2. Execute statistical analyses with professional statistical software.
3. Demonstrate skill in data management for cyber security and forensic.
4. apply data science concepts and methods to solve problems in real-world contexts
5. Understand the practical case studies in cyber securities and forensic

Course Contents:

1. Data for Cyber Security and Forensic
2. Understanding Data Analysis and Visualization
3. Data Analysis for Cybersecurity and forensic
4. Data Analysis for Cybersecurity and forensic
5. Case Studies / Applications

Laboratory Exercises:

1. Python Basic programming
2. Data Preprocessing using Python Libraries
3. Basic Statistics using Python
4. Simple Linear Regression
5. Classification using Naive Bays
6. Clustering Using K-Means
7. Data Visualization using Python

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Learning Resources:

Text Books:

1. Cathy O'Neil, Rachel Schutt, Doing Data Science, Straight Talk from The Frontline. O'Reilly, 2013
2. Applied Statistics And Probability For Engineers – By Douglas Montgomery.
3. Jiawei Han, Micheline Kamber, Jian Pei, "Data Mining: Concepts and Techniques", 3rd Edition

Reference Books:

1. Foundations of Data Science By Avrim Blum, John Hopcroft, and Ravindran Kannan
2. Ward, Grinstein Keim, Interactive Data Visualization: Foundations, Techniques, and Applications. Natick: A K Peters, Ltd.
3. Glenn J. Myatt, Making sense of Data: A practical Guide to Exploratory Data Analysis and Data Mining, John Wiley Publishers, 2007.

Supplementary Reading:

https://swayam.gov.in/nd1_noc19_cs60/preview

Web Resources:

https://nptel.ac.in/courses/106/106/106106179/

Weblinks:

https://www.youtube.com/watch?v=MiiANxRHSv4
https://www.youtube.com/watch?v=y8Etr3Tx6yE&list=PLyqSpQzTE6M_JcleDbrVyPnE0PixKs2JE&index=5

MOOCs:

https://intellipaat.com/data-scientist-course-training/
https://www.coursera.org/learn/python-programming-intro

Pedagogy:

1. Power Point Presentation
2. Two Teacher Method
3. Video Lectures
4. Flipped Classroom Activity
5. Group Discussion
6. Chalk and Boar

Assessment Scheme:

Class Continuous Assessment (CCA): 30 marks

Mid Term	Component 1 (Active Learning)	Component 2
15 Marks	10 Marks	5 Marks

Laboratory Continuous Assessment (LCA): 30 marks

Practical Performance	Active Learning/Mini Project/ Additional Implementation/On paper Design	End term Practical/ Oral Examination
10 Marks	10 Marks	10 Marks

Term End Examination: 40 Marks

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Dr. Dinesh Seth
Dean

Syllabus: Theory

Module No.	Contents	Workload in Hrs. Theory
1	**Data for Cyber Security and Forensic** Type of data encountered in CSF, Synthetic v/s real-world data, Data discovery and classification ,outliers, incident reporting Assessing quality of data sets, Big Data , Cloud Computing, Business Intelligence, Cleansing unstructured data ,Data security strategies	09
2	**Understanding Data Analysis and Visualization** Statistics for Data science , How is data analytics used in cybersecurity? Review, analyse, and draw conclusions from data. Apply quantified mathematical models to appropriate variables for data analysis, Creating data visualizations to better present information	09
3	**Data Analysis for Cybersecurity and forensic,** Types of Data-driven security approaches, Categories, Challenges in Data Analysis, Data Description, Ground Truth, Extracting Indicators, Algorithmic poisoning, Discovering malicious URL's, Big Data, use of Big Data for detecting attacks, detect host scanning,	09
4	**Data Analysis for Cybersecurity and forensic** Systematic Analysis of cyber security using data, threats and attacks on various layers, threats and attacks on various devices, Ensuring Information Privacy, Anomaly detection, Adversarial Machine Learning, Deep Neural Networks (DNN), Game theoretic approaches	09
5	**Case Studies / Applications**	09

Laboratory:

Module No.	Contents	Workload in Hrs. Lab
1	Python Basic Programming	04
2	Data Preprocessing using Python Libraries	04
3	Basic Statistics using Python	04
4	Simple Linear Regression	04
5	Classification using Naive Bays	04
6	Clustering Using K-Means	04
7	Data Visualization using Python	04

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Dr. Vishwanath Karad
MIT WORLD PEACE UNIVERSITY PUNE

COURSE STRUCTURE

Course Code	**CET4037B**			
Course Category	**Professional Elective**			
Course Title	**Cyber Physical Security**			
Teaching Scheme and Credits	**Lecture**	**Tutorial**	**Laboratory**	**Credits**
Weekly load hrs	**3**	**-**	**2**	**3+0+1=4**

Pre-requisites:

- Computer network
- Information security
- Programming experience with C and Python

Course Objectives:

1. **Knowledge**:
   i. Describe what cyber-physical systems are
2. **Skills**
   i. Demonstrate what makes cyber-physical systems hard to secure
   ii. Analyze common methods used to secure cyber-physical systems
3. **Attitude**:
   i. Evaluate the differences between securing traditional enterprise systems and cyber-physical systems

Course Outcomes:

After completion of the course the students will be able to :-

1. Develop the ability to interact with cyber-physical systems components
2. Develop the ability to interact with cyber-physical systems protocols
3. Develop the ability to conduct attacks on cyber-physical systems protocols and systems
4. Develop the ability to design cyber-physical systems and architectures that are resilient to attack

Course Contents:

1. Internet of Things (IoT)
2. Industrial Internet
3. Smart Cities
4. Smart Grid

Learning Resources:

Text Books:

1. Industrial Network Security, Second Edition: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems (2nd Edition), by Eric D. Knapp and Joel Thomas Langill, ISBN: 978-0124201149
2. Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure (1st Edition), by Eric D. Knapp and Raj Samani, ISBN: 978-1597499989

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Reference Books:

1. Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions (1st Edition), by Clint Bodungen, Bryan Singer, Aaron Shbeeb, Kyle Wilhoit, and Stephen Hilt, ISBN: 978-1259589713.

Pedagogy:

- Power Point Presentation
- Two Teacher Method
- Video Lectures
- Flipped Classroom Activity

Assessment Scheme:

Class Continuous Assessment (CCA) - 30 Marks

Mid Term	Component 1 (Active Learning)	Component 2	Total
15	10	5	30

Laboratory Continuous Assessment (LCA) 30 marks

Practical Performance	Active learning / Mini Project/Additional implementation/ On paper design	End term practical /oral examination	Total
10	10	10	30

End Term Exam: 40 Marks

Theory Syllabus:

Module No.	Contents	Workload in Hrs.
1	**Foundations of Cyber-Physical System Security** Introduction to Cyber-Physical Systems, Overview of CPS, Networking, Information Security Control Systems. CPSS: Concepts and Principles, Security Breaches and Defenses in CPS, Cyber Physical Systems in Real world, Basic Principle of Cyber Physical Systems, Industry 4.0, IIoT, Cyber Physical Systems Design Recommendations, CPS system requirements, Cyber Physical System Application.	10
2	**Industrial Networks** Industrial Networks, Industrial Cyber Security History and Threats, Introduction to Industrial Control Systems And Operations, Ladder Logic, Industrial Network Design and Architecture, Industrial Network Protocols, Hacking & Securing Industrial Control Systems, Power Delivery Systems (Example Industrial Control System).	10

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Dr. Dinesh Seth
Dean

3	**Cyber Physical System – Models and Dynamics Behaviours** Continuous Dynamics, Discrete dynamics, Hybrid Systems. **Study of Embedded Systems vs Internet of Things vs Cyber Physical System** Design of Embedded Systems (I/O Units, Multitasking and Scheduling), Internet of Things Architecture, CPS Architecture	07
4	**Control System Security** Security and Privacy Issues in CPSs, Local Network Security for CPSs, Internet-Wide Secure Communication, Threats to Cyber-Physical Systems in Other Domains, Securing Industrial Control Systems, Privacy in Cyber-Physical Systems, Threats to Cyber-Physical Systems in Other Domains, CPSS: Legal and Privacy Aspects, Risk Management, CPSS and Cyberwarfare, Case Study: Cybersecurity in Digital Manufacturing/Industry 4.0.	09
5	**Case Study** Smart Energy Grids SERS, Healthcare. Automotive Cyber physical Systems, VANET, Automatic cruise control. Robot Interaction in a cloud environment.	09

Laboratory:

Module No.	Contents	Workload in Hrs.
1	Setting up Raspberry-pi and arduino interface for building a Cyber Physical system	2
2	Basic Input/ Output GPIO and analog Interface in Microcontrollers	2
3	Working with sensors through an I/O Interface	4
4	Building a Cyber Physical System Model using Matlab	2
5	Building a PID based Cyber Physical System model for maintaining room temperature	2
6	Building a Cyber physical system model for Adaptive cruise control in vehicle	2
7	Building an effective security system for a CPS	2
8	Building IoT based communication model for connecting devices	2

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Dr. Vishwanath Karad
MIT WORLD PEACE UNIVERSITY | PUNE

COURSE STRUCTURE

Course Code	CET4038B			
Course Category	Professional Elective			
Course Title	Security Platforms and Tools			
Teaching Scheme and Credits	Lecture	Tutorial	Laboratory	Credits
Weekly load hrs	3 hrs./week	-	2 hrs./week	3+0+1=04

Pre-requisites:

- Computer Networks
- Information Security

Course Objectives:

1. Knowledge

i) To study various security platforms for enterprise security solutions

2. Skills

i) To study various cyber security tools focused for specific problems

3. Attitude

i) To understand application and cyber security testing tools

Course Outcomes:

After completion of the course the students will be able to :-

1. Compare and demonstrate security platforms for suitable secured applications
2. Apply cyber security tools to achieve specific security goals
3. Experiment and analyze cyber security testing tools

Course Contents:

1. Security Platforms and Tools
2. Security Platforms Case Study
3. Cyber Security Tools
4. Security Testing Tools I
5. Security Testing Tools II

Learning Resources:

Text Books:

1. Nitesh Dhanjani & Justin Clarke, Network Security Tools: Writing, Hacking, and Modifying Security Tools, Oreilly Publications
2. Hardeep Singh, Kali Linux Wireless Pentesting and Security for Beginners, rootsh311.com
3. John Sherwood & Andrew Clark & David Lynas, Enterprise security architecture : a business-driven approach, CRC press

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
Date 08 JUN 2023

Supplementary Reading:

Web Resources:

- https://www.tutorialspoint.com/security_testing/index.htm
- https://www.trendmicro.com/en_us/what-is/cybersecurity-platform.html
- https://technologymagazine.com/articles/top-10-cyber-security-platforms
- https://www.infosys.com/services/cyber-security/offerings/platform-powered-services.html
- https://www.fortinet.com/
- https://www.ibm.com/security
- https://www.checkpoint.com/cyber-hub/cyber-security/what-is-a-cyber-security-architecture/what-is-enterprise-security-architecture/
- https://www.isaca.org/resources/isaca-journal/issues/2017/volume-4/enterprise-security-architecturea-top-down-approach

MOOCs:

- https://www.coursera.org/learn/introduction-cybersecurity-cyber-attacks
- https://www.coursera.org/projects/web-application-security-testing-with-owsap-zap
- https://nptel.ac.in/courses/106106178
- https://www.udemy.com/course/enterprise-security-fundamentals-d/
- https://www.udemy.com/course/enterprise-information-security-management-part2/?kw=security+tools&src=sac
- https://www.udemy.com/course/cyber-security-in-9-steps/?kw=security+tools&src=sac

Pedagogy:

- Power Point Presentation
- White-board / Pen
- Mini Projects/ Quizzes / Sudden tests
- Seminar / Activity/ Assignments

Assessment Scheme:

Class Continuous Assessment (CCA): 30 Marks

Theory Assignments	Active Learning	Mid Term Test
05 Marks	10 Marks	15 Marks

Laboratory Continuous Assessment (LCA): 30 Marks

LCA performance	LCA Activity	LCA orals
10	10	10

Term End Examination: 40 Marks

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Dr. Dinesh Seth
Dean

Syllabus:

Module Number	Content	Workload in Hrs.
1	**Introduction to Security Platforms** Need for Security platforms, Types of Security Platforms, Enterprise Security Architecture, Principles, Benefits, Security domains- ISO27001. Jfrog Security platform study, Infosys Cyber Next study, The Forrester Wave-Data Security Platform, Fortinet Security Platform: Network Security, Enterprise Networking, Endpoint Security, Security Operations, Operational Technology, Application Security, Device Security.	9
2	**Security Platform Case Study** **CISCO Security Platform:** Advanced Malware Protection (AMP), Cloud and Application Security, Email Security, Endpoint Security, Firewalls, Network Security, Network Visibility and Segmentation, Next-Generation Intrusion Prevention System (NGIPS), Security Management, Security Platform, VPN and Endpoint Security Clients, Vulnerability Management, Web Security, Workload Security, Industrial Security for IOT, OT & ICS, User and Device Security.	9
3	**Cyber Security Tools** Types of Security tools: Penetration testing, Packet sniffers, Encryption, Scanning web vulnerability, Network defenses, Network security monitoring, Detecting network intrusions, Anti Virus. Nmap, Metasploit, Wireshark, Nessus, Firewall , Snort, Burp suite, Nikto, Aircrack-ng, John the Ripper, Cain and Abel, Nikto, Kali Linux, Splunk, Antivirus software, OSSEC, TrueCrypt, KeePass, Nagios, KisMAC, NetStumbler, Bitdefender, Encryption software, Forcepoint, Tcpdump, NESSUS, IPTables. Acunetix, Lifelock, AxCrypt, OSSIM, GNU-PG.	9
4	**Security Testing Tools I** Security Testing Tools- Overview, Process, Malicious Software, HTTP Protocol Basics, HTTPS Protocol Basics, Encoding and Decoding, Cryptography, Same Origin Policy, Cookies, Hacking Web Applications, Injection Testing tools, Broken Authentication, Testing Cross Site Scripting, Insecure Direct Object Reference, Testing Security Misconfiguration, Tools for Sensitive Data Exposure. Security policy management Tools, Security Audit Tools, DevSecOps tools	9
5	**Security Testing Tools II** Missing Function Level Access Control, Cross Site Request Forgery tools, Components with Vulnerabilities tools, Unvalidated Redirects and Forwards tools, Ajax Security tools, Web Service tools, Buffer Overflows tools, Denial of Service, Testing Malicious File Execution tools, Automation Tools	9

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
Date 08 JUN 2023

Laboratory:

Sr. No.	Title of Laboratory (Any 10 Laboratories)	Workload in Hrs.
1	Case study of Information Security Platform such as Infosys, CISCO etc.	2
2	Case study of Enterprise Information Security	2
3	Demonstration of Intrusion detection and Alerting Mechanism tool	2
4	Installation and configuration of Security Auditing tool	2
5	Installation and configuration of Security Policy Management tool	2
6	Demonstration of Penetration Testing and reporting	2
7	Use any software security testing tool and demonstrate it analysis	2
8	Demonstrate network security monitoring tool	2
9	Demonstrate Broken Authentication using OWASP Webgoat tool	2
10	Demonstrate Security Misconfiguration using OWASP Webgoat tool	2
11	Study of burp Suite community edition tool to find security flaws	2
12	Study of Metasploit security tool	2
13	Study of OSSEC tool based intrusion detection system	2
14	Study of OpenVAS is a security testing suite for vulnerability assessment	2
15	Demonstrate any DevSecOps tools	2

Dr. Dinesh Seth
Dean

MIT-WPU
Approved by
Academic Council
Date 8...JUN/...2023

Dr. Vishwanath Karad
MIT WORLD PEACE UNIVERSITY PUNE
TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

MIT-WPU

COURSE STRUCTURE

Course Code	CET2009B			
Course Category	**Project**			
Course Title	**Mini Project**			
Teaching Scheme and Credits	**Lectures**	**Tutorial**	**Laboratory**	**Credits**
Weekly load hrs	–	-	**2 hr/week**	0+1=1

Pre-requisites:

- Programming Skills
- Software Engineering and Project Management

Course Objectives:

1. To apply the knowledge of fundamental concepts learned during the curriculum to formulate the problem statement and develop a computer based system using appropriate algorithms
2. To examine and utilize modern skills, techniques and tools for computing practice leading to lifelong learning
3. To incorporate SDLC to identify appropriate processes, components and make use of modern engineering tools to evaluate, test and analyze the developed computer based system
4. To understand key ethical and social issues while reaching optimum solution for the problem statement and demonstrate work ethics in teams to effectively manage conflicts
5. To present ideas and concepts clearly in an organized manner

Course Outcomes:

On completion of course, students should be able to:

1. Demonstrate the ability to apply knowledge of fundamental concepts to formulate the problem statement and find optimum solution
2. Analyze a problem and identify the computing requirements for its solution
3. Design and develop computer based systems by making use of appropriate modern \ engineering tools.
4. Resolve key ethical and social issues affecting the problem statement and demonstrate team Ethics.
5. Present ideas and concepts clearly in an organized manner

Assessment Scheme:

The students are directed to form groups and all members of the group jointly work towards the implementation of the mini project. The selection of the mini project and topic finalization is based on the approval of the review committee. Every group is required to work towards the aims and objectives to well define the problem statement. For the same they will perform literature survey and propose an architecture/high level design of the mini project. The group will develop the working module of the proposed design with appropriate analysis and results of the system or subsystem in the area of Computer Science and Engineering.

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Dr. Dinesh Seth
Dean

The term work evaluation will be done by the review team in consultation with the guide. Oral presentation will be based on the mini project work completed by the candidates.

Laboratory Continuous Assessment (LCA)-100 Marks

Practical Performance	Active learning / Mini Project/Additional implementation/ On paper design	End Term practical/ Oral Examination
30 marks	40 marks	30 marks

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Dr. Dinesh Seth
Dean

Dr. Vishwanath Karad
MIT WORLD PEACE UNIVERSITY | PUNE
TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

COURSE STRUCTURE

Course Code	CET3008B			
Course Category	**Project**			
Course Title	**Seminar**			
Teaching Scheme and Credits	**Lectures**	**Tutorial**	**Laboratory**	**Credits**
Weekly load hrs	–	-	**2 hr/week**	0+1=1

Course Objectives:

1. Knowledge:
   a. To learn the basic principles of communication with active, empathetic listening, speaking and writing techniques.
2. Skills:
   a. To explore research with new technologies.
   b. To build independent thinking on real-time issues.
3. Attitude:
   a. To use presentation standards and guidelines effectively.

Course Outcomes:

On completion of the course, student will be able –

6. To grasp the technical skills with writing, reading, analysis, visuals and inhibit good communication skills.
7. To write a technical report summarizing state-of-the-art on an identified topic.
8. To use multiple thinking strategies to examine real-world issues.
9. To explore and enhance the use of various presentation tools and techniques.

Assessment Scheme:

The students will have to deliver the seminar on any technical state-of-the-art topic approved by the guide. The presentation should cover introduction, motivation, literature survey, mathematical modeling, data-table discussion (if applicable) and conclusion and future work. It is appreciated and strongly recommended that the student should select the domain of his/her seminar and identify the literature confined to the domain. Thorough literature study based on the broad identified topic has to be carried out. Selection of seminar topic in multidisciplinary domain will be strongly recommended and supported.

To bring the quality and appropriateness of the seminar work it is mandatory for the seminar guides to maintain a progressive record of the meetings. During meeting with the seminar guides, it is expected that it should include the discussion agenda, weekly outcomes achieved, corrective actions and comments on the progress report as per the plan submitted by the students.

The reports should be prepared using MSdoc/Latex application tool and submitted in the school.

MIT-WPU
Approved by
Academic Council
Date 08/JUN/2023

Dr. Dinesh Seth
Dean

Laboratory Continuous Assessment (LCA)-100 Marks

Practical Performance	Active learning / Mini Project/Additional implementation/ On paper design	End Term practical/ Oral Examination
30 marks	40 marks	30 marks

SOP Seminar:

1. Identify the Faculties to be eligible as Seminar guides.
2. Mapping the expertise of the Seminar guides with the respective domains.
3. The identified domains are communicated to the students.
4. Each student is instructed to submit at least 03 seminar topics as per the domain list.
5. The Seminar ideas are scrutinized by domain experts.
6. One of the idea is selected with its feasibility, current scenario, etc. and the topic is finalized. First review R1 for the Seminars is conducted by a panel of Seminar Coordinators.
7. The Seminar title and the Seminar guide is communicated to the students.
8. The students are required to report to their guides on a weekly basis and maintain a log book for the same. Log book is a record of the discussions and decisions taken collaboratively by the guides and the students.
9. The students incorporate the suggestions from R1 and accordingly design/ devise the details to be presented in review R2.
10. Final Seminar submission includes complete documentation of the Seminar Report.
11. Seminar Report consists of Technical Contents-Literature Review, Research gap study, Methodology/Techniques, Conclusion, Applications, References etc.)
12. Plagiarism check to be performed before submitting the final Seminar Report.
13. Students may also submit/publish a journal/conference paper on the state-of-art-study.
14. It is mandatory to all students to actively participate & attend all the Seminar sessions.
15. Final evaluation of the Seminars, review R3 is conducted by a panel of domain experts.

MIT-WPU
Approved by
Academic Council
08 JUN 2023
Date...../...../.....

Dr. Dinesh Seth
Dean