IV Year - I Semester

S.No	Category	Course Code	Course Title	L	T	P	C	IM	EM	TM
1	PE	UGCS7T2422 UGCS7T2522 UGCS7T2622 UGCS7T2722 UGCS7T2822	**Professional Elective-III** 1. Information Security Analysis & Audit 2. Penetration Testing & Vulnerability Analysis 3. IOT Security 4. Database Security 5. Computer Forensics	3	-	-	3	30	70	100
2	PE	UGCS7T2922 UGCS7T3022 UGCS7T3122 UGCS7T3222 UGCS7T3322	**Professional Elective-IV** 1. Information Security Management 2. Malware Analysis 3. Cloud Security 4. Mobile & Wireless Security 5. Darknet and Deep Web	3	-	-	3	30	70	100
3	PE	UGCS7T3422 UGCS7T3522 UGCS7T3622 UGCS7T3722	**Professional Elective-V** 1. Information Security Incident Response 2. Cyber Laws & Ethics 3. Cyber Crime Investigation 4. Web Application Security	3	-	-	3	30	70	100
4	OE/JOE	UGCS7T1322 UGCS7T1422 UGCS7T0222 UGCS7T0422	**Job Oriented Elective-I** 1. Augmented Reality and Virtual Reality 2. Big Data Analytics 3. Dart Programming 4. DevOps	2	-	2	3	30	70	100
5	OE/JOE	UGCS7T1722 UGCS7T0822 UGCS7T1922 UGCS7T2022	**Job Oriented Elective-II** 1. Blockchain Technologies 2. Artificial Intelligence 3. Go Programming 4. Robotic Process Automation	2	-	2	3	30	70	100
6	HSSE	UGMB7T0122	Management Science	3	-	-	3	30	70	100
7	SOC	UGCS7K2122 UGCS7K2222 UGCS7K3822 UGCS7K3922	Amazon Web Services Game Development Data Visualization Bug Bounty Hunting	1	-	2	2	50	-	50
8	Internship	UGCS7I2322	Industrial/Research Internship(After third year)	-	-	-	3	50	-	50
			Total	**17**	**0**	**6**	**23**	**280**	**420**	**700**
Honors/Minor Course (4 Credits)										

IV Year - II Semester

S.No	Category	Course Code	Course Title	L	T	P	C	IM	EM	TM
1	Major Project	UGCS8J0122	Major Project & Internship (6 Months)	-	-	20	10	60	140	200
2	Seminar	UGCS8S0222	Seminar	-	2	-	2	50	-	50
			Total	**0**	**2**	**20**	**12**	**110**	**140**	**250**

L – Lectures, T – Tutorials, P – Practicals, C – Credits, IM – Internal Marks, EM – External Marks, TM – Total Marks

BS - Basic Science, HSS - Humanities & Social Science, ES - Engineering Science, MC - Mandatory Course, PC - Professional Core, SOC - Skill Oriented Course, OE/JOE - Open Elective/Job Oriented Elective, PE - Professional Elective, HSSE - Humanities & Social Science Elective

IV Year
I Semester

INFORMATION SECURITY ANALYSIS & AUDIT
(Professional Elective-III)

	L	T	P	C
Subject Code: UGCS7T2422	**L**	**T**	**P**	**C**
IV Year / I Semester	**3**	**0**	**0**	**3**

Prerequisites: Basic knowledge on Information Security.

Course objectives: This course helps in Studying the instances affecting system security to gain knowledge about possible fixes and countermeasures to frequent risks and vulnerabilities. To familiarize with Security Audits for the existing systems.

SYLLABUS:

UNIT: (10 Hours)

Information Security Fundamentals: Definitions & challenges of security, Attacks & services, Security policies, Security Controls, Access control structures, Cryptography, Deception, Ethical Hacking, Firewalls, Identify and Access Management (IdAM).

UNIT-II (10 Hours)

System Security: System Vulnerabilities, Network Security Systems, System Security, System Security Tools, Web Security, Application Security, Intrusion Detection Systems.

UNIT-III (10 Hours)

Information Security Management: Monitor systems and apply controls, security assessment using automated tools, backups of security devices, Performance Analysis, Root cause analysis and Resolution, Information Security Policies, Procedures, Standards and Guidelines.

Incident Management: Security requirements, Risk Management, Risk Assessment, Security incident management, third party security management, Incident Components, Roles.

UNIT-IV (10 Hours)

Incidence Response: Incident Response Lifecycle, Record, classify and prioritize information security incidents using standard templates and tools, Responses to information security incidents, Vulnerability Assessment, Incident Analysis.

UNIT-V (10 Hours)

Conducting Security Audits: Common issues in audit tasks and how to deal with these, Different systems and structures that may need information security audits and how they operate, including: servers and storage devices, infrastructure and networks, application hosting and content management, communication routes such as messaging, Features, configuration and specifications of information security systems and devices and associated processes and architecture, Common audit techniques, Record and report audit tasks, Methods and techniques for testing compliance.

Information Audit Preparation: Establish the nature and scope of information security audits, Roles and responsibilities, Identify the procedures/guidelines/checklists, Identify the requirements of information security, audits and prepare for audits in advance, Liaise with appropriate people to gather data/information required for information security audit.

Course Outcomes:

Upon completion of this course, the students will be able to

CO1: Contribution for managing information security and coordinating information security incidents

CO2: Contribution for the information security Audits

CO3: Empowering teams prepared for and undertake information security audits

CO4: Developing the knowledge, Skill & Competence for information security audit

Mapping of COs to POs:

POs/ COs	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2
CO1	2	-	2	-	-	-	-	-	-	-	-	-	-	-
CO2	2	3	2	3	-	-	-	-	-	-	-	-	-	-
CO3	2	3	2	3	-	-	-	-	-	-	-	-	-	-
CO4	2	3	3	-	-	-	-	-	-	-	-	-	-	-

TEXT BOOKS:

1.William Stallings, Lawrie Brown, Computer Security: Principles and Practice, 3rd edition, 2014.

2. Nina Godbole, Information Systems Security: Security Management, Metrics, Frameworks and Best Practices, Wiley, 2017

3. Nina Godbole, Sunit Belapure, Cyber Security- Understanding cyber-crimes, computer forensics and legal perspectives, Wiley Publications, 2016

4. Andrew Vladimirov Michajlowski, Konstantin, Andrew A. Vladimirov, Konstantin V. Gavrilenko, Assessing Information Security: Strategies, Tactics, Logic and Framework, IT Governance Ltd, O?Reilly, 2010

REFERENCE BOOKS:

1. Charles P. Pfleeger, Security in Computing, 4th Edition, Pearson, 2009.

2. Christopher J. Alberts, Audrey J. Dorofee , Managing Information Security Risks, Addison-Wesley Professional

3. Peter Zor, The Art of Computer Virus Research and Defense, Pearson Education Ltd, 2005

4. Lee Allen, Kevin Cardwell, Advanced Penetration Testing for Highly-Secured Environments - Second Edition, PACKT Publishers, 2016

PENETRATION TESTING & VULNERABILITY ANALYSIS
(Professional Elective-III)

Subject Code: UGCS7T2522	**L**	**T**	**P**	**C**
IV Year / I Semester	**3**	**0**	**0**	**3**

Prerequisites: Basic knowledge on Python and Ethical Hacking.

Course Objectives:

1. To learn the tools that can be used to perform information gathering.
2. To identify various attacks in various domains of cyber space.
3. To learn about exploits in various operating systems and Wireless environment.
4. To learn how vulnerability assessment can be carried out by means of automatic tools or manual investigation.
5. To learn the vulnerabilities associated with various network applications and database system.

Syllabus:

UNIT I: (8 Hours)

Information Gathering and Detecting Vulnerabilities: Open Source Intelligence Gathering - Port Scanning - Nessus Policies - Web Application Scanning Manual Analysis- Traffic Capturing.

UNIT II: (9 Hours)

Attacks: Password Attacks Client side Exploitation Social Engineering- Bypassing Antivirus Applications.

Exploits: Metasploit Payloads Open phpMyAdmin -Buffer overflow: Windows and Linux, Web scanning exploits, port scanning exploits, SQL exploits

UNIT III: (12 Hours)

Wireless Security: Wired vs. wireless Privacy Protocols - Wireless Frame Generation - Encryption Cracking Tools - Wireless DoS Attacks.

Network Vulnerability Analysis: Domain Name Server and Dynamic Host Configuration Protocol -Light Weight Directory Access Protocol-Simple Network Management Protocol, Remote Procedural Call

UNIT IV: (8 Hours)

Common Vulnerability Analysis of Application Protocols: Simple Mail Transfer Protocol, File Transfer Protocol- Trivial File Transfer Protocol-Hyper Text Transmission Protocol-ICMP SMURF- UDP-DNS-PING-SYN

UNIT V: **(8 Hours)**

Penetration Tools and Database Security: Trace routes, Neotrace, Whatweb. Database Security: Access control in database systems – Inference control-Multilevel database security.

Course Outcomes:

Upon completion of this course, the students will be able to:

CO1: Ability to determine the security threats and vulnerabilities in computer networks using Penetration testing techniques

CO2: Set up of a hacking lab environment to study and document vulnerabilities within the network.

CO3: Realize and respect ethical boundaries to demonstrate and understand what is necessary and appropriate when conducting penetration tests.

Mapping of COs to POs:

POs/ COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO 10	PO 11	PO 12
CO1	3	3	-	-	3	-	-	-	-	-	3	-
CO2	3	3	-	-	-	-	-	-	-	-	-	-
CO3	3	3	-	-	-	3	-	-	-	-	-	-

TEXT BOOKS:

1. Georgia Weidman, Penetration Testing: A Hands On Introduction to Hacking, No Startch Press, First Edition 2014.
2. B.Singh, H.Joseph and Abhishek Singh,"Vulnerability Analysis and Defense for the Internet, Springer, 2008 Edition

REFERENCE BOOKS:

1. RafayBaloch, "EthicalHacking and Penetration Testing Guide",CRC Press, 2015
2. Dr.Patrick Engebretson, "The Basics of Hacking and Penetration Testing",Syngress Publications Elseveir, 2013.
3. Prakhar Prasad, Mastering Modern Web Penetration Testing (Kindle Edition),2016 , Packt Publishing.
4. Gilberto Najera Gutierrez, Kali Linux Web Penetration Testing Cookbook,2016.
5. Robert Svensson, From Hacking to Report Writing: An Introduction to Security and Penetration Testing, 2016.

IOT SECURITY
(Professional Elective-III)

	L	T	P	C
Subject Code: UGCS7T2622	**L**	**T**	**P**	**C**
IV Year / I Semester	**3**	**0**	**0**	**3**

Prerequisites: Basic knowledge on IOT and Information Security.

Course Objectives: To learn about the security issues in IOT. To learn about the Security Architecture in the IOT.To learn about the security measures taken in IOT.

Syllabus:

UNIT – I :

SECURING THE INTERNET OF THINGS : (10 Hours)

Introduction – Security Requirements in IoT architectures – Security in Enabling Technologies – IoT Security Life Cycle – Cryptographic Fundamentals for IoT Security Engineering - Security Concerns in IoT Applications.

UNIT- II : **(10 Hours)**

SECURITY ARCHITECTURE IN THE INTERNET OF THINGS: Introduction– Security Requirements in IoT – Insufficient Authentication/Authorization – Insecure Access Control – Threads to Access Control, Privacy, and Availability – Attacks Specific to IoT – Malware Propagation and Control in Internet of Things.

UNIT- III: (10 Hours)

PRIVACY PRESERVATION : Privacy Preservation Data Dissemination - Privacy Preservation for IoT used in Smart Building – Exploiting Mobility Social Features for Location Privacy Enhancement in Internet of Vehicles – Lightweight and Robust Schemes for Privacy Protection in Key personal IOT Applications: Mobile WBSN and Participatory Sensing.

UNIT- IV : (10 Hours)

TRUST, AUTHENTICATION AND DATA SECURITY: Trust and Trust Models for IoT – Emerging Architecture Model for IoT Security and Privacy – preventing Unauthorized Access to Sensor Data – Authentication in IoT – Computational Security for the IoT – Security Protocols for IoT Access Network.

UNIT- V : (10 Hours)

SOCIAL AWARENESS AND CASE STUDIES: User Centric Decentralized Governance Framework for Privacy and Trust in IoT – Security and Impact of the IoT on Mobile Networks – Security Concerns in Social IoT – Security for IoT Based Healthcare.

COURSE OUTCOMES:

Upon completion of this course, the students will be able to

CO1: Describe the basics of securing the Internet of Things.(L2)

CO2: Understand architecture and threats in IoT. (L2)

CO3: Compare various privacy schemes related to IoT (L4)

CO4: Describe the authentication mechanisms for IoT security and privacy.(L2)

CO5: Examine security issues for various applications using case studies.(L4)

Mapping of COs to POs:

POs/ COs	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12
CO1	3	2	-	-	-	-	-	-	-	-	-	-
CO2	3	-	3	-	-	-	-	-	-	-	-	-
CO3	3	2	3	3	-	-	-	-	-	-	-	-
CO4	3	3	3	-	-	-	-	-	-	-	-	-
CO5	3	3	-	3	-	-	-	-	-	-	-	2

TEXT BOOKS:

1. Shancang Li, Li Da Xu, "Securing the Internet of Things" , 1st edition,2017.
2. Arsheep Bahga , Vijay Madisetti, "INTERNET OF THINGS - A HANDS-ON APPROACH", 2015.
3.Sridipta Misra, Muthucumaru Maheswaran, Salman Hashmi, "Security Challenges and Approaches in Internet of Things," Springer, 2016.
4. Drew Van Duren, Brian Russell, "Practical Internet of Things Security", Packt, 1st Edition, 2016.

REFERENCE BOOKS:

1. Fei Hu, "Security and Privacy in Internet of Things (IoTs)", 1st edition, 2016.

DATABASE SECURITY
(Professional Elective-III)

Subject Code: UGCS7T2722	**L**	**T**	**P**	**C**
IV Year / I Semester	**3**	**0**	**0**	**3**

Prerequisites: Basic knowledge on database concepts and information security.

Course Objectives: To study the different models involved in database security and their applications in real time world to protect the database and information associated with them.

Syllabus:

UNIT I: (9 Hours)

Introduction to Databases Security: Problems in Databases Security Controls, Security Models.

Introduction Access Matrix Model: Take-Grant Model, Acten Model, PN Model, Hartson and Hsiao's Model, Fernandez's Model, Bussolati and Martella's Model for Distributed databases.

UNIT II: (11 Hours)

Security Models: Bell and LaPadula's Model, Biba's Model, Dion's Model, Sea View Model, Jajodia and Sandhu's Model, The Lattice Model for the Flow Control conclusion, Security Mechanisms, Introduction User Identification/Authentication, Memory Protection, Resource Protection, Control Flow Mechanisms, Isolation Security Functionalities in Some Operating Systems, Trusted Computer System Evaluation Criteria.

UNIT III: (13 Hours)

Security Software Design: Introduction, A Methodological Approach to Security Software Design, Secure Operating System Design, Secure DBMS Design, Security Packages Database Security.

Design Statistical Database Protection & Intrusion Detection Systems Introduction Statistics Concepts and Definitions, Types of Attacks, Inference Controls evaluation Criteria for Control Comparison.
Introduction, IDES System, RETISS System, ASES System Discovery.

UNIT IV: (8 Hours)

Models For The Protection Of New Generation Database Systems -1 Introduction, A Model for the Protection of Frame Based Systems, A Model for the

Protection of Object Oriented Systems, SORION Model for the Protection of Object-Oriented Databases.

UNIT V: (8 Hours)

Models For The Protection Of New Generation Database Systems - 2

A Model for the Protection of New Generation Database Systems: the Orion Model Jajodia and Kogan's Model, A Model for the Protection of Active Databases Conclusions.

Course Outcomes:

Upon completion of this course, the students will be able to:

CO1: Identify the Problems in Databases Security Controls [L2]

CO2: Recognize the unauthorized data and Avoid unauthorized data modification.[L2]

CO3: Demonstrate the data confidentiality and Prove that the data integrity is preserved [L3]

CO4: Distinguish the various Models For the Protection Of New Generation Database Systems [L4]

Mapping of COs to POs:

POs/ COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO 10	PO 11	PO 12
CO1	3	2	1	-	-	-	-	2	2	1	-	1
CO2	3	3	2	2	1	-	-	2	2	1	-	2
CO3	3	3	3	1	1	-	-	2	2	1	-	2
CO4	3	3	2	2	1	-	-	3	3	1	-	2

TEXT BOOKS:

1. Database Security and Auditing, Hassan A. Afyouni, India Edition, CENGAGE Learning, 2009.
2. Database Security, Castano, Second edition, Pearson Education.

REFERENCE BOOKS:

1.Database security by alfred basta, melissa zgola, CENGAGE learning

COMPUTER FORENSICS
(Professional Elective-III)

Subject Code: UGCS7T2822	**L**	**T**	**P**	**C**
IV Year / I Semester	**3**	**0**	**0**	**3**

Prerequisites: Basic knowledge of operating systems, programming, hacking techniques and malware.

Course Objectives: This course helps students to

- Correctly define and cite appropriate instances for the application of computer forensics correctly collect and analyze computer forensic evidence.
- Identify the essential and up-to-date concepts, algorithms, protocols, tools, and methodology of Computer Forensics.

Syllabus:

UNIT I: **(9 Hours)**

Computer Forensics Fundamentals: What is Computer Forensics?, Use of Computer Forensics in Law Enforcements, Computer Forensics Assistance to Human Resources/Employment Proceedings, Computer Forensics Services, Benefits of professional Forensics Methodology, Steps taken by Computer Forensics Specialists.

Types of Computer Forensics Technology: - Types of Business Computer Forensic Technology. Types of Military Computer Forensic Technology, Types of Law Enforcement- Computer Forensic Technology, Types of Business Computer Forensic Technology.

Computer Forensics Evidence and capture: Data Recovery Defined-Data Back-up and Recovery-The Role of Back-up in Data Recovery-The Data Recovery Solution.

UNIT II: **(9 Hours)**

Evidence Collection and Data Seizure: Why Collect Evidence? Collection Options- Obstacles-Types of Evidence-The Rules of Evidence-Volatile Evidence-General Procedure-Collection and Archiving-Methods of Collections-Art facts-Collection Steps-Controlling Contamination: The chain of custody.

Duplication and Preservation of Digital Evidence: Preserving the Digital Crime Scene-Computer Evidence processing steps-Legal Aspects of collecting and Preserving Computer forensic Evidence.

Computer image Verification and Authentication: Special needs of Evidential Authentication - Practical Consideration-Practical Implementation.

UNIT III: **(11 Hours)**

Computer forensic analysis and validation: Determining what data to collect and analyze, validating forensic data, addressing data-hiding techniques, performing remote acquisitions.

Network Forensics: Network forensic overview, performing live acquisitions, developing standard procedures for network forensics, using network tools, examining the honey net project.

Processing crime at incident scenes: Identifying digital evidence, collecting evidence in private-sector incident scenes, processing law enforcement crime scenes, preparing for a search, securing a computer incident or crime scene, seizing digital evidence at the scene, storing digital evidence, obtaining a digital hash, reviewing a case.

UNIT IV: (8 Hours)

Current Computer Forensic Tools: evaluating computer forensic tool needs, computer forensic software tools, computer forensic hardware tools, validating and testing forensic software.

E-mail investigations: Exploring the role of email in investigations, exploring the role of client and server in email, investigating email crimes and violations, understanding email servers, using specialized email forensic tools.

Cell phone and mobile device forensics: Understanding mobile device forensic, understanding acquisition procedures for cell phones and mobile devices.

UNIT V: (8 Hours)

Computer forensic cases: Developing Forensic Capabilities – Searching and Seizing Computer Related Evidence –Processing Evidence and Report Preparation – Future Issues.

Course Outcomes:

Upon completion of this course, the students will be able to:

CO1: Understand the basic terminology and basics of computer forensics. [L2]

CO2: Analyze and validate digital evidence data. [L4]

CO3: Use Different Computer forensic tools to a given scenario. [L3]

CO4: Examine computer forensic cases. [L4]

Mapping of COs to POs:

POs/ COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO 10	PO 11	PO 12
CO1	3	3	3	3	3	3	-	-	-	-	-	3
CO2	3	3	3	3	3	3	-	-	-	-	-	3
CO3	3	3	3	3	3	3	-	-	-	-	-	3
CO4	3	3	3	3	3	3	-	-	-	-	-	3

TEXT BOOKS:

1. Computer Forensics, Computer Crime Investigation by John R,Vacca, Firewall Media, New Delhi.
2. Marjie T Britz, "Computer Forensics and Cyber Crime: An Introduction",Pearson Education, 2nd Edition, 2008.
3. Computer Forensics and Investigations by Nelson, Phillips Enfinger, Steuart, CENGAGE Learning.

REFERENCE BOOKS:

1. Real Digital Forensics by Keith j.Jones, Richard Bejitlich,Curtis W.Rose ,Addison-Wesley, Pearson Education
2. Forensic Compiling, A Tractitioneris Guide by Tony Sammes and Brain Jenkinson, Springer International edition.
3. Computer Evidence Collection &Presentation by Christopher L.T. Brown,Firewall Media.
4. Homeland Security, Techniques& Technologies by Jesus Mena,Firewall Media.
5. Software Forensics Collecting Evidence from the Scene of a Digital Crime by Robert M.Slade, TMH 2005
6. Windows Forensics by chad Steel,Wiley India Edition.

INFORMATION SECURITY MANAGEMENT
(Professional Elective-IV)

Subject Code: UGCS7T2922	**L**	**T**	**P**	**C**
IV Year / I Semester	**3**	**0**	**0**	**3**

Prerequisites: Knowledge on TCP/IP, Cryptography and Network security.

Course Objectives:

An Information Security Management is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process. It can help small, medium and large businesses in any sector keep information assets secure.

Syllabus:

Unit I **(8 Hours)**

Information Security Management: Information Security Overview, Threats and Attack Vectors, Types of Attacks, Common Vulnerabilities and Exposures (CVE), Security Attacks, Fundamentals of Information Security, Computer Security Concerns, Information Security Measures etc.

Unit II **(9 Hours)**

Fundamentals of Information Security: Key Elements of Networks, Logical Elements of Network, Critical Information Characteristics, Information States etc.

Unit III **(8 Hours)**

Data Leakage: What is Data Leakage and statistics, Data Leakage Threats, Reducing the Risk of Data Loss, Key Performance Indicators (KPI), Database Security etc.

Unit IV **(10 Hours)**

Information Security Policies, Procedures and Audits: Information Security Policies-necessity-key elements & characteristics, Security Policy Implementation, Configuration, Security Standards-Guidelines & Frameworks etc.

Unit V **(10 Hours)**

Information Security Management — Roles and Responsibilities: Security Roles & Responsibilities, Accountability, Roles and Responsibilities of Information Security Management, team-responding to emergency situation-risk analysis process etc.

Course Outcomes:

Upon completion of this course, the students will be able to:

CO1: Understand the concepts of information security, types of threats and attacks and information Security Measures [L2]

CO2: Understand the key Elements and Logical Elements of Networks and various information states [L3]

CO3: Apply the principles in designing solutions to manage security risks effectively.[L3]

CO4: Understand the Information Security Policies, Guideline and Framework of Information Security standards.[L3]

CO5: Understand the Roles and Responsibilities of ISM [l2]

Mapping of COs to POs:

POs/ COs	**PO 1**	**PO 2**	**PO 3**	**PO 4**	**PO 5**	**PO 6**	**PO 7**	**PO 8**	**PO 9**	**PO 10**	**PO 11**	**PO 12**
CO1	3	3	3	3	-	-	-	-	-	-	-	-
CO2	3	3	2	2	-	-	-	-	-	-	-	-
CO3	3	3	3	2	-	-	-	-	-	2	-	-
CO4	3	3	3	2	-	-	-	-	-	-	-	-
CO5	2	2	3	3						-		

TEXT BOOKS:

1. Management of Information Security by Michael E.Whitman and Herbert J.Mattord

REFERENCE BOOKS:

1. http://www.iso.oronso/homeistandards/management-standards/iso27001.htm
2. httpellcsrc.nist.00v/bublicationsinistoubs/800-55-Rev1/SP800-55-rev1.pdf

MALWARE ANALYSIS
(Professional Elective-IV)

	L	T	P	C
Subject Code:UGCS7T3022	**L**	**T**	**P**	**C**
IV Year / I Semester	**3**	**0**	**0**	**3**

Prerequisites: Basic knowledge on Networks and security.

Course Objectives: To introduce the malware taxonomy and malware analysis tools. Also to identify and analyze malware samples using static, dynamic analysis, and reverse engineering techniques, and to detect and analyze malicious documents and mobile malware.

Syllabus:

UNIT I: **(9 Hours)**

Fundamentals of Malware Analysis: Malware taxonomy - Malware analysis techniques – Packed and Obfuscated Malware - Portable Executable File Format: Headers and Sections, Malware Analysis in Virtual Machines - Malware Analysis Tools: ProcMon/ ProcExplore, BinText, FileAlyzer, OllyDbg, etc..

UNIT II: **(9 Hours)**

Static Analysis: File signature analysis and Identifying file dependencies -Database of file hashes. String analysis - Local and online malware sandboxing - Levels of Abstraction - x86 Architecture -x86/x86_64 Assembly - Static Analysis Tools: PeiD, Dependency Walker, Resource Hacker.

UNIT III: **(12 Hours)**

Dynamic Analysis: Source level vs. Assembly level Debuggers - Kernel vs. User-Mode Debugging – Exceptions - Modifying Execution with a Debugger - Modifying Program Execution in Practice - DLL analysis - Dynamic Analysis Tools: Virustotal, Malware Sandbox, Windows Sysinternals.

Reverse Engineering: Reverse engineering malicious code - Identifying malware passwords - Bypassing authentication - Advanced malware analysis: Virus, Trojan and APK Analysis - Reverse Engineering Tools: IDA Pro and OLLYDBG.

UNIT IV: **(10 Hours)**

Malicious Document Analysis: PDF and Microsoft Office document structures – Identify PDF and office document vulnerabilities - Analysis of suspicious websites - Examining malicious documents: word, XL, PDF, and RTF files - Malware extraction and analysis tools.

Anti-Reverse-Engineering: Anti-Disassembly - Anti-Debugging - Anti-Forensic Malware - Packers and Unpacking – Shellcode Analysis - 64-Bit Malware

UNIT V: (10 Hours)

Mobile Malware Analysis: Mobile application penetration testing - Android and iOS Vulnerabilities - Exploit Prevention - Handheld Exploitation - Android Root Spreading and Distribution Android Debugging - Machine learning techniques for malware analysis: Support Vector Machine (SVM), K-Nearest Neighbor (KNN), Random Forest (RF), Decision Trees (DT), Naïve Bayes (NB), and Neural Networks (NN).

Course Outcomes:

Upon completion of this course, the students will be able to:

CO1: Possess the skills to carry out static and dynamic malware analysis on various malware samples[L2].

CO2: Understand the executable formats, Windows internals, and APIs. [L3]

CO3: Apply techniques and concepts to unpack, extract, and decrypt malware. [L3]

CO4: Comprehend reverse-engineering of malware and anti-malware analysis. [L4]

CO5: Achieve proficiency with industry-standard malware analysis tools.[L4]

Mapping of COs to POs:

POs/ COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO 10	PO 11	PO 12
CO1	3	3	3	-	-	-	-	-	-	-	-	-
CO2	3	3	-	-	-	-	-	-	-	-	-	-
CO3	3	-	3	-	-	-	-	-	-	-	-	-
CO4	3	3	3	-	-	-	-	-	-	-	-	-
CO5	3	3	-	-	-	-	-	-	-	-	3	-

TEXT BOOKS:

1. Abhijit Mohanta, Anoop Saldanha, Malware Analysis and Detection Engineering a Comprehensive Approach to Detect and Analyze Modern Malware, 2020, 1st edition.
2. M. Sikorski and A. Honig, Practical Malware Analysis: The Hands-on Guide to Dissecting Malicious Software. 2012, 1st edition.

REFERENCE BOOKS:

1. MonnappaK A, Learning Malware Analysis- Explore the concepts, tools, and techniques to analyze and investigate Windows malware, 2018, 1st edition.
2. Practical Malware Analysis – The Hands–On Guide to Dissecting Malicious Software – Michael Sikorski.

CLOUD SECURITY
(Professional Elective-IV)

	L	T	P	C
Subject Code:UGCS7T3122	**L**	**T**	**P**	**C**
IV Year / I Semester	**3**	**0**	**0**	**3**

Prerequisites: Basic knowledge on cloud computing and information security.

Course Objectives: This course aims cloud computing security concepts. Student will examine the security and compliance benefits of using the public cloud and will explore access control and access management features of public cloud platform. Additionally, the course covers the Cloud governance and rules.

Syllabus:

UNIT I: (10 Hours)

Security Concepts: Confidentiality, privacy, integrity, authentication, non-repudiation, availability, access control, Concepts implementation and relevance in the cloud computing, and their importance in PaaS, IaaS and SaaS. e.g. User authentication in the cloud; Relevant cloud security design principles; least privilege, separation of duties, Defence in Depth, Fail Safe, Economy of Mechanism, Complete Mediation, Open Design, Least Common Mechanism, Weakest Link.

UNIT II: (9 Hours)

Cloud and Security concepts: Cloud Data Security, Cloud Data Life Cycle; Create, Store, Use, Share, Archive, Destroy, Cloud Storage Architectures; Volume Storage, Object based storage, databases, Content Delivery Network(CDN), Cloud Data Security Foundation Strategies; Encryption, Masking, Obfuscation, Anonymization, Tokenization, Security Information and Event Management, Egress Monitoring(DLP).

UNIT III: (9 Hours)

Cloud Issues and Testing: Shared Cloud Platforms Risks and Responsibilities, Cloud Computing Risks by Deployment and service model, Cloud Attack Surface, Threats by deployment model, Cloud Security Policy Implementation issues and Decomposition, NIST 33 Security Principles, Cloud Penetration Testing; Legal and ethical implications, The three pre-test phases, Usage of various tools including Tenable.io(Vulnerability Management, Web Application Scanning & Container Security) and other penetration testing tools.

UNIT IV: (10 Hours)

Cloud Security and Management: Cloud Secure Software Development Life Cycle, ISO/IEC 27034-1 Standards for Secure Application, Single Sign On (SSO), Federated Identity Management, Federation Standards, Multifactor Authentication, Cloud Application Architecture; Secure APIs, Tenancy Separation, Cryptography, Sandboxing, Application Virtualization, Runtime Application Self Protection (RASP).

UNIT V: (11 Hours)

VM Security and Responsibilities: VM Life Cycle; Overwriting, Degaussing, Destruction, Record Retention, Data Remanence, Virtualization Security Management, Virtual Threats, Hypervisor Risks, Increased Denial of Service Risks, VM Security Recommendations, Storage Operations, Physical and Logical Isolation, Basic Operational Application Security, Threat Modelling, Application Testing Methods, Change and Configuration Management, Business Continuity and Disaster Recovery, Incident Response, NISTSpecial Publication 800-61, Responsibility, ownership of data, Right to penetration test, local lawwhere data is held, Examination of modern Security Standards (e.g. PCIDSS, ISO 27001).

Course Outcomes:

Upon completion of this course, the students will be able to:

CO1: To learn and examine the security breaches of IaaS, PaaS and SaaS [L3].

CO2: Apply various data encryption methods and security mechanisms to get the administrative control using IAM service. [L3]

CO3: Create a secure production environment using cloud security features and services. [L3]

CO4: Virtualization Security and management with right penetration.[L4]

Mapping of COs to POs:

POs/ COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO 10	PO 11	PO 12
CO1	3	3	-	-	-	-	-	-	-	-	-	-
CO2	3	3	-	-	-	-	-	-	-	-	-	-
CO3	3	3	-	-	-	-	-	-	-	-	-	-
CO4	3	3	3	-	-	-	-	-	-	-	-	-

TEXT BOOKS:

1. Tim Mather, Subra Kumaraswamy, Shahed Latif, “Cloud Security and Privacy: An EnterprisePerspective on Risks and Compliance” O'Reilly Media; 1 edition, 2009.
2. Ronald L. Krutz, Russell Dean Vines, “Cloud Security”, 2010.
3. John Rittinghouse, James Ransome, “Cloud Computing” CRC Press; 1 edition, 2009

REFERENCE BOOKS:

1. Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing”.
2. Vmware “VMware Security Hardening Guide” White Paper, June 2011.
3. Cloud Security Alliance 2010, “Top Threats to Cloud Computing” Microsoft 2013.

MOBILE AND WIRELESS SECURITY
(Professional Elective-IV)

	L	T	P	C
Subject Code: UGCS7T3222	**L**	**T**	**P**	**C**
IV Year / I Semester	**3**	**0**	**0**	**3**

Prerequisites: Basic knowledge on Mobile Computing and Computer Networks.

Course Objectives: The purpose of this course is to equip the students with the skills needed to protect and recover computer systems & networks from a variety of security threats.

Syllabus:

UNIT I: (9 Hours)
Security Issues in Mobile Communication: Mobile Communication History, Security – Wired Vs Wireless, Security Issues in Wireless and Mobile Communications, Security Requirements in Wireless and Mobile Communications, Security for Mobile Applications, Advantages and Disadvantages of Application – level Security.

UNIT II: (9 Hours)
Security of Device, Network, and Server Levels: Mobile Devices Security Requirements, Mobile Wireless network level Security, Server Level Security. Application Level Security in Wireless Networks: Application of WLANs, Wireless Threats, Some Vulnerabilities and Attach Methods over WLANs, Security for 1G Wi-Fi Applications, Security for 2G Wi-Fi Applications, Recent Security Schemes for Wi-Fi Applications

UNIT III: (12 Hours)
Application Level Security in Cellular Networks: Generations of Cellular Networks, Security Issues and attacks in cellular networks, GSM Security for applications.
GPRS Security for applications, UMTS security for applications, 3G security for applications, Some of Security and authentication Solutions.

UNIT IV: (9 Hours)
Application Level Security in MANETs: MANETs, Some applications of MANETs, MANET Features, Security Challenges in MANETs, Security Attacks on MANETs, External Threats for MANET applications, Internal threats for MANET Applications, Some of the Security Solutions.

Ubiquitous Computing: Need for Novel Security Schemes for UC, Security Challenges for UC, and Security Attacks on UC networks, Some of the security solutions for UC.

UNIT V: (10 Hours)

Data Center Operations: Security challenge, implement "Five Principal Characteristics of Cloud Computing, Data center Security Recommendations Encryption for Confidentiality and Integrity, Encrypting data at rest, Key Management Lifecycle, Cloud Encryption Standards.

Course Outcomes:

Upon completion of this course, the students will be able to:

CO 1: Familiarize with the issues and technologies involved in designing a wireless and mobile system that is robust against various attacks. [L2]

CO 2: Gain knowledge and understanding of the various ways in which wireless networks can be attacked and tradeoffs in protecting networks. [L2]

CO 3: Have a broad knowledge of the state-of-the-art and open problems in wireless and mobile security, thus enhancing their potential to do research or pursue a career in this rapidly developing area. [L3]

CO 4: Learn various security issues involved in cloud computing. [L3]

CO 5: Learn various security issues related to GPRS and 3G. [L2]

Mapping of COs to POs:

POs/ COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO 10	PO 11	PO 12
CO1	1	-	-	-	-	-	-	-	-	-	-	-
CO2	1	-	-	-	-	-	-	-	-	-	-	-
CO3	3	-	-	-	-	-	-	-	-	-	-	-
CO4	3	-	-	-	-	-	-	-	-	-	-	-
CO5	1	-	-	-	-	-	-	-	-	-	-	-

TEXT BOOKS:

1. Pallapa Venkataram, Satish Babu: "Wireless and Mobile Network Security", 1st Edition, Tata McGraw Hill,2010.
2. Frank Adelstein, K.S.Gupta : "Fundamentals of Mobile and Pervasive Computing", 1st Edition, Tata McGraw Hill 2005.

REFERENCE BOOKS:

1. Randall k. Nichols, Panos C. Lekkas : "Wireless Security Models, Threats and Solutions", 1st Edition, Tata McGraw Hill, 2006.
2. Bruce Potter and Bob Fleck : "802.11 Security" , 1st Edition, SPD O'REILLY 2005.

3. James Kempf: “Guide to Wireless Network Security, Springer. Wireless Internet Security – Architecture and Protocols”, 1st Edition, Cambridge University Press, 2008.

DARKNET AND DEEP WEB
(Professional Elective-IV)

	L	T	P	C
Subject Code: UGCS7T3322				
IV Year / I Semester	**3**	**0**	**0**	**3**

Prerequisites: Basic knowledge on Computer Networks.

Course Objectives:

a) Perform security self-assessments by understanding concepts
b) Differentiate between deep, dark, and surface web
c) Understand laws, regulations, and privacy considerations
d) Identify common uses based on real-world events
e) Build an anonymous web for secure communications utilizing publicly available tools
f) Identify multi-dimensional threats

Syllabus:

UNIT I: **(9 Hours)**

Introduction to the Darknet and Deep Web: Understanding the surface web, deep web, and darknet, Historical context and evolution of the Darknet, Anonymity and privacy on the internet.

Accessing the Darknet: Tor network and its architecture, setting up and configuring the Tor Browser, Alternative networks (I2P, Freenet).

UNIT II: **(10 Hours)**

Navigating the Darknet: Popular Darknet marketplaces and forums, Hidden wikis and directories, Search engines for the Darknet.

Cryptocurrencies and Anonymity: Bitcoin and other cryptocurrencies on the Darknet, Anonymizing transactions, The role of cryptocurrencies in illicit activities.

UNIT III: **(12 Hours)**

Darknet Marketplaces: Types of products and services available, Security and trust issues, Case studies of prominent marketplaces.

Darknet Communities and Forums: Forums, discussion boards, and social media platforms on the Darknet, Subcultures and ideologies within Darknet communities. The role of anonymity in online discourse.

UNIT IV: **(9 Hours)**

Darknet Threats and Risks: Cybercrime and hacking on the Darknet, Scams, fraud, and malware distribution, staying safe while exploring the Darknet.

Law Enforcement and Legal Aspects: Law enforcement efforts to combat Darknet activities, Legal cases and prosecutions related to the Darknet, International collaboration and challenges.

UNIT V: (9 Hours)

Ethics of the Darknet: Ethical considerations when researching or using the Darknet, the role of anonymity in protecting human rights activists and whistleblowers, Debates on the ethical use of the Darknet.

Darknet and Cybersecurity: Darknet as a source of threat intelligence, Vulnerabilities and exploits found on the Darknet, Strategies for defending against Darknet threats.

Course Outcomes:

Upon completion of this course, the students will be able to:

CO1: Ability to set up and configure the Tor Browser, access Darknet websites, and use other tools for secure and anonymous browsing. [L2]

CO2: Analyze and evaluate the credibility of information found on the Darknet, discerning between reliable sources and potentially harmful content. [L3]

CO3: Able to take ethical decisions when faced with potential ethical dilemmas related to the Darknet and Deep Web. [L3]

CO4: Understanding the best practices for online security and privacy when navigating the Darknet, including protecting personal information. [L1]

Mapping of COs to POs:

POs/ COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO 10	PO 11	PO 12
CO1	3	-	-	-	-	-	-	-	-	-	-	-
CO2	-	3	-	-	-	-	-	-	-	-	-	-
CO3	-	-	3	-	-	-	-	-	-	-	-	-
CO4	3	3	-	-	-	-	-	-	-	-	-	-

TEXT BOOKS:

1. The Dark Net by Jamie Bartlett, 2015
2. Dark Web: Exploring and Data Mining the Dark Side of the Web, 2011.

REFERENCE BOOKS:

1. Darknet Master: Tor and Deep Web Secrets by Warren Wake.
2. Tor and the Deep Web: Bitcoin, Darknet & Cryptocurrency: Encryption & Online Privacy for Beginners by Lance Henderson.

INFROMATION SECURITY INCIDENT RESPONSE
(Professional Elective-V)

	L	T	P	C
Subject Code: UGCS7T3422	**L**	**T**	**P**	**C**
IV Year / I Semester	**3**	**0**	**0**	**3**

Prerequisites: Networking fundamentals, operating systems and cyber security concepts.

Course Objectives:

1. Understand the principles of incident response, including incident identification, containment, eradication, and recovery.
2. Develop the skills to effectively analyze and respond to security incidents, such as malware infections, data breaches, and denial-of-service attacks.
3. Gain hands-on experience in incident handling through simulations and practical exercises

Syllabus:

UNIT I: (9 Hours)

Introduction to Incident Response: Overview of incident response principles and practices, Incident classification and severity assessment, Legal and ethical considerations in incident response.

UNIT II: (9 Hours)

Incident Identification and Detection: Techniques for identifying and detecting security incidents, Intrusion detection systems (IDS) and security information and event management (SIEM), Incident response playbooks and procedures.

UNIT III: (10 Hours)

Incident Containment and Eradication: Strategies for containing and eradicating security threats, Isolation of affected systems and networks, Malware analysis and removal techniques.

UNIT IV: (9 Hours)

Incident Recovery and Communication: Developing incident recovery plans, Communication with stakeholders, including management and law enforcement, Post-incident review and reporting.

UNIT V: (9 Hours)

Hands-On Incident Response: Practical exercises and simulations of security incidents, Use of incident response tools and technologies, Incident debriefing and lessons learned.

Course Outcomes:

By the end of this course, students should be able to:

CO1. Identify and classify security incidents, including malware infections, intrusions, and data breaches.

CO2. Develop and execute incident response plans to contain, eradicate, and recover from security incidents.

CO3. Utilize incident response tools and techniques to investigate and mitigate security breaches.

CO4. Collaborate effectively in incident response teams and communicate findings to stakeholders.

CO5. Apply ethical and legal principles in handling security incidents and protecting sensitive data.

Mapping of COs to POs:

POs/ COs	**PO 1**	**PO 2**	**PO 3**	**PO 4**	**PO 5**	**PO 6**	**PO 7**	**PO 8**	**PO 9**	**PO 10**	**PO 11**	**PO 12**
CO1	3	-	-	-	-	-	-	-	-	-	-	3
CO2	-	3	-	-	-	-	-	-	-	-	-	-
CO3	-	-	3	-	-	-	-	-	-	-	-	-
CO4	-	-	-	3	-	-	-	-	-	-	-	-
CO5	-	-	-	-	-	3	-	3	-	-	-	-

TEXT BOOKS:

1. "Incident Response & Computer Forensics" by Chris Prosise and Kevin Mandia
2. "Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response" by Leighton Johnson

REFERENCE BOOKS:

1. "Incident Response: A Strategic Guide to Handling System and Network Security Breaches" by E. Eugene Schultz and Russell Shumway
2. "The Practice of Network Security Monitoring: Understanding Incident Detection and Response" by Richard Bejtlich

CYBER LAWS & ETHICS
(Professional Elective-V)

	L	T	P	C
Subject Code: UGCS7T3522	**L**	**T**	**P**	**C**
IV Year / I Semester	**3**	**0**	**0**	**3**

Prerequisites: Basic knowledge on Information Security.

Course Objectives: This course explores technical, legal, and social issues related to cybercrimes, Laws Cyber Ethics. Cybercrime and laws is a broad term that includes offences where a computer may be the target, crimes where a computer may be a tool used in the commission of an existing offence, and crimes where a computer may play a subsidiary role such as offering evidence for the commission of an offence. It is also required to have knowledge of Cyber Ethics and its role and significance.

Syllabus:

UNIT I: **(9 Hours)**

Introduction to Cyber law: Evolution of computer Technology, emergence of cyber space. Cyber Jurisprudence, Jurisprudence and law, Doctrinal approach, Consensual approach, Real Approach, Cyber Ethics, Cyber Jurisdiction, Hierarchy of courts, Civil and criminal jurisdictions, Cyberspace Web space, Web hosting and web Development agreement, Legal and Technological Significance of domain Names, Internet as a tool for global access.

UNIT II: **(8 Hours)**

Information Technology Act: Overview of IT Act, 2000, Amendments and Limitations of IT Act, Digital Signatures, Cryptographic Algorithm, Public Cryptography, Private Cryptography, Electronic Governance, Legal Recognition of Electronic Records, Legal Recognition of Digital Signature, Certifying Authorities, Cyber Crime and Offences, Network Service Providers Liability, Cyber Regulations Appellate Tribunal, Penalties and Adjudication.

UNIT III: **(12 Hours)**

Cyber law and Related Legislation: Patent Law, Trademark Law, Copyright, Software – Copyright or Patented, Domain Names and Copyright disputes, Electronic Data Base and its Protection, IT Act and Civil Procedure Code, IT Act and Criminal Procedural Code, Relevant Sections of Indian Evidence Act, Relevant Sections of Bankers Book Evidence Act, Relevant Sections of Indian Penal Code, Relevant Sections of Reserve Bank of India Act, Law Relating To Employees And Internet, Alternative Dispute Resolution, Online Dispute Resolution (ODR).

UNIT IV: **(8 Hours)**

Electronic Business and legal issues: Evolution and development in E-commerce, paper vs paper less contracts E-Commerce models- B2B, B2C, E security. Business, taxation, electronic payments, supply chain, EDI, E-markets, Emerging Trends.

UNIT V: **(8 Hours)**

Cyber Ethics: The Importance of Cyber Law, Significance of cyber Ethics, Need for Cyber regulations and Ethics. Ethics in Information society, Introduction to Artificial Intelligence Ethics: Ethical Issues in AI and core Principles, Introduction to Block Chain Ethics.

Course Outcomes:

Upon completion of this course, the students will be able to:

CO1: Understand importance of professional practice, Cyber Law and Ethics in their personal lives and professional careers. [L2]

CO2: Dissect Information Technology act and Related Legislation. [L4]

CO3: Demonstrate Electronic business and legal issues. [L2]

CO4: Interpret Cyber Ethics, rights and responsibilities as an employee, team member and a global citizen. [L5]

Mapping of COs to POs:

POs/ COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO 10	PO 11	PO 12
CO1	3	3	3	-	-	-	-	-	-	-	-	-
CO2	3	3	3	-	-	-	-	-	-	-	-	-
CO3	3	3	3	-	-	-	-	-	-	-	-	-
CO4	3	3	3	-	-	-	-	-	-	-	-	-

TEXT BOOKS:

1. Cyber Laws: Intellectual property & E Commerce, Security - Kumar K, dominant Publisher
2. Cyber Ethics 4.0, Christoph Stuckelberger, Pavan Duggal, by Globethic
3. Information Security policy & Implementation Issues, NIIT, PHI

REFERENCE BOOKS:

1. Computers, Internet and New Technology Laws, Karnika Seth, Lexis Nexis Butterworths Wadhwa Nagpur.
2. Legal Dimensions of Cyber Space, Verma S, K, Mittal Raman, Indian Law Institute, New Delhi,
3. Cyber Law, Jonthan Rosenoer, Springer, New York, (1997).
4. The Information Technology Act, 2005: A Handbook, OUP Sudhir Naib,, New

York, (2011)

5. Information Technology Act, 2000, S. R. Bhansali,, University Book House Pvt. Ltd., Jaipur (2003).
6. Cyber Crimes and Law Enforcement, Vasu Deva, Commonwealth Publishers, New Delhi, (2003).

CYBER CRIME INVESTIGATION
(Professional Elective-V)

Subject Code: UGCS7T3622	**L**	**T**	**P**	**C**
IV Year / I Semester	**3**	**0**	**0**	**3**

Prerequisites: Basic knowledge on Cyber Security.

Course Objectives: This course helps students to understand various types of cyber-attacks, cyber-crimes, learn threats and risks within context of the cyber security and overview of the cyber laws.

Syllabus:

UNIT I: (9 Hours)

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

UNIT II: (8 Hours)

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

UNIT III: (12 Hours)

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

UNIT IV: (8 Hours)

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

UNIT V: (8 Hours)

Laws and Acts: Laws and Ethics, Digital Evidence Controls, Evidence Handling Procedures, Basics of Indian Evidence ACT IPC and CrPC, Electronic Communication Privacy ACT, Legal Policies.

Course Outcomes:

Upon completion of this course, the students will be able to:

CO1: Understand the fundamentals of cybercrime and issues. [L2]

CO2: Understand different investigation tools for cybercrime. [L2]

CO3: Demonstrate how to draft a digital forensics report for the appropriate audience. [L2]

CO4: Analyze different laws, ethics and evidence handling procedures [L3]

Mapping of COs to POs:

POs/ COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO 10	PO 11	PO 12
CO1	3	3	-	-	-	-	-	-	-	-	-	-
CO2	3	3	-	-	-	-	-	-	-	-	-	-
CO3	3	3	-	-	-	-	-	-	-	-	-	-
CO4	3	3	-	-	-	-	-	-	-	-	-	-

TEXT BOOKS:

1. Nelson Phillips and Enfinger Steuart, "Computer Forensics and Investigations", Cengage Learning, New Delhi, 2009.
2. Kevin Mandia, Chris Prosise, Matt Pepe, "Incident Response and Computer Forensics ", Tata McGraw -Hill, New Delhi, 2006.
3. Moore, Robert, (2011). Cybercrime, investigating high-technology computer crime (2nd Ed.). Elsevier

REFERENCE BOOKS:

1.https://www.bu.edu/online/programs/certificate-programs/cybercrime-investigation-cybersecurity/.

2. Robert M Slade," Software Forensics", Tata McGraw - Hill, New Delhi, 2005.
3. Bernadette H Schell, Clemens Martin, "Cybercrime", ABC – CLIO Inc, California, 2004.
4. "Understanding Forensics in IT ", NIIT Ltd, 2005.
5. Cyber Crime Investigations, Anthony Reyes, Syngress Publishing, Inc (2007).

WEB APPLICATION SECURITY
(Professional Elective-V)

Subject Code: UGCS7T3722	**L**	**T**	**P**	**C**
IV Year / I Semester	**3**	**0**	**0**	**3**

Prerequisites: Networking Fundamentals, Web Development Basics and Cyber security Fundamentals.

Course Objectives: This course aims to provide students with a fundamental understanding of web application security principles, common vulnerabilities, and security best practices.

Syllabus:

UNIT I: (9 Hours)
Introduction to Web Application Security: Introduction to web application security concepts, Importance of web application security, Threat landscape and security challenges in web applications, The role of security in the software development lifecycle.

UNIT II: (9 Hours)
Web Application Vulnerabilities: Common web application vulnerabilities (e.g., SQL injection, XSS, CSRF), Understanding attack vectors and exploitation techniques, Real-world examples of web application breaches and their impact, Introduction to the OWASP Top Ten Project.

UNIT III: (10 Hours)
Secure Coding Practices: Principles of secure coding for web applications, Input validation and sanitization, Authentication and authorization mechanisms, Session management and secure communication, Error handling and logging.

UNIT IV: (9 Hours)
Web Application Security Testing: Manual and automated security testing techniques, Vulnerability scanning and assessment tools, Security testing methodologies (e.g., black-box, white-box, gray-box testing), Reporting and remediation of security findings.

UNIT V: (9 Hours)
Web Application Firewall (WAF) and Incident Response: Introduction to Web Application Firewalls (WAF), Deploying and configuring WAF for web application protection, Incident response and handling security breaches, Web application security monitoring and alerting.

Course Outcomes:

Upon completion of this course, the students will be able to:

CO1- Identify and analyze web application security vulnerabilities.

CO2- Apply secure coding practices to develop and maintain web applications.

CO3- Perform security testing and assessment on web applications.

CO4- Configure and manage Web Application Firewalls (WAFs) for protection.

CO5- Develop an incident response plan for web application security breaches.

Mapping of COs to POs:

POs/ COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO 10	PO 11	PO 12
CO1	3	-	-	-	-	-	-	-	-	-	-	3
CO2	-	3	-	-	-	-	-	-	-	-	-	-
CO3	-	-	3	-	-	-	-	-	-	-	-	-
CO4	-	-	-	3	-	-	-	-	-	-	-	-
CO5	-	-	-	-	-	3	-	3	-	-	-	-

TEXT BOOKS:

1. "Web Application Security: A Beginner's Guide" by Bryan Sullivan, Vincent Liu
2. "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" by Dafydd Stuttard and Marcus Pinto
3. "Secure Coding in C and C++" by Robert C. Seacord (For secure coding practices)
4. "OWASP Testing Guide" by The OWASP Foundation (Free online resource for security testing)

REFERENCE BOOKS:

1. Web Application Security: Threats, Countermeasures, and Best Practices" by Lakshmanan Ganapathy and Mike Ware
2. Hacking Web Apps: Detecting and Preventing Web Application Security Problems" by Mike Shema
3. Secure Programming with Static Analysis" by Brian Chess and Jacob West

AUGMENTED REALITY AND VIRTUAL REALITY
(JOB ORIENTED ELECTIVE-I)

	L	T	P	C
Subject Code: UGCS7T1322	**L**	**T**	**P**	**C**
IV Year / I Semester	**2**	**0**	**2**	**3**

Prerequisites: Basic knowledge on programming and computer graphics.

Course Objectives:
To introduce the basic concepts of Augmented Reality and Virtual Reality and to gain knowledge on various devices required for interaction and applications.

Syllabus:

UNIT I: **(8 Lectures)**

Introduction: Virtual Reality, Augmented Reality, Mixed Reality, Augmented Virtuality, Extended Reality, History, VR Features, VR Controllers, Current issues with VR, AR Mobile devices, AR headsets, AR glasses, AR Controllers, Current issues with AR.

UNIT II: **(8 Lectures)**

Consuming Content in VR : High-end devices, Mid-tier devices, Low-end devices, Near-Future Hardware.

Consuming Content in AR: Microsoft HoloLens, Meta 2, Magic Leap, Mira Prism, Apple ARKit, Google ARCore, Near-Future Hardware.

UNIT III: **(12 Lectures)**

Creating Content in VR and AR: Evaluating Your Project, Planning Your Virtual Reality Project, Planning Your Augmented Reality Project, Assessing Design Software, Capturing Real Life, Assessing Development Software, Distributing Your Content.

Cross-Platform Theory: Role of Game Engines, Understanding 3D Graphics, The Virtual Camera, Degrees of Freedom, Portability Lessons from Video Game Design, Simplifying the Controller Input.

UNIT IV: **(8 Lectures)**

Virtual Reality Toolkit: History of VRTK, SteamVR Unity Toolkit, VRTK v4, Future of VRTK, Success of VRTK, Getting Started with VRTK 4.

Best Practices: Handling Locomotion in VR & AR, Effective Use of Audio in VR & AR, Common Interactions Paradigms, Inventory for VR, Augmented Reality Raycasts.

UNIT V: **(8 Lectures)**

Applications: Travel, Museums, Aerospace, Retail, Military, Education, Entertainment, Real Estate, Advertising and Marketing, Mobile Apps for Experiencing Augmented Reality, Future of Virtual Reality and Augmented Reality.

Course Outcomes:

Upon completion of this course, the students will be able to:

CO 1. Gain knowledge on AR & VR and various components involved in manifesting the same.

CO 2. Plan content creation and identify necessary software required in implementing AR & VR.

CO 3. Analyze the portability issues and understand the best practices.

CO 4. Understand how to implement various applications using AR and VR technologies.

Mapping of COs to POs:

POs/ COs	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2
CO1	3	-	-	-	-	-	-	-	-	-	-	-	-	-
CO2	3	-	3	-	-	-	-	-	-	-	-	-	-	-
CO3	3	-	3	-	3	-	-	-	-	-	-	-	-	-
CO4	3	3	3	-	3	-	-	-	-	-	-	-	3	-

TEXT BOOKS:

1. Paul Mealy, Virtual & Augmented Reality For Dummies, John Wiley & Sons, Inc
2. Erin Pangilinan, Steve Lukas and Vasanth Mohan, Creating Augmented and Virtual Realities, O'Reilly Media Inc.

REFERENCE BOOKS:

1. Kelly S. Hale, Kay M. Stanney, Handbook of Virtual Environments: Design, Implementation, and Applications, Second Edition, CRC Press.
2. Gregory C. Burdea & Philippe Coiffet, John, Virtual Reality Technology, Second Edition, Wiley & Sons, Inc.
3. William R.Sherman, AlanCraig, Understanding Virtual Reality, interface, Application and Design, Elsevier (Morgan Kaufmann).
4. John Vince, Virtual Reality Systems, Pearson Education.
5. Andrew Davison, Killer Game Programming in Java, Oreilly-SPD.
6. Alan B Craig, William R Sherman and Jeffrey D Will, "Developing Virtual Reality Applications: Foundations of Effective Design", Morgan Kaufmann.
7. Alan B. Craig, Understanding Augmented Reality, Concepts and Applications, Morgan Kaufmann
8. Steve Aukstakalnis, "Practical Augmented Reality: A Guide to the Technologies, Applications, and Human Factors for AR and VR", Addison Wesley.
9. Brett S. Martin, "Virtual Reality", Norwood House Press.
10. Anand R., "Augmented and Virtual Reality", Khanna Publishing House, Delhi
11. Adams, "Visualizations of Virtual Reality", Tata McGraw Hill.

BIG DATA ANALYTICS
(JOB ORIENTED ELECTIVE-I)

Subject Code: UGCS7T1422	**L**	**T**	**P**	**C**
IV Year / I Semester	**2**	**0**	**2**	**3**

Prerequisites: Knowledge of high level programming languages and SQL for analyzing the data.

Course Objectives: The student will be able to understand Big Data as a popular term used to describe the exponential growth, availability and use of information, both structured and unstructured. It is imperative that organizations and IT leaders focus on the ever-increasing volume, variety and velocity of information that forms Big Data. Hadoop is the core platform for structuring BigData, and solves the problem of making it useful for Analytics.

Syllabus:

UNIT I: **(8 Lectures)**

Introduction to Big Data: What is Big Data and where it is produced? Rise of Big Data, Compare Hadoop vs traditional systems, Limitations and Solutions of existing Data Analytics Architecture, Attributes of Big Data, Types of Data, Use Cases of Big Data, Other technologies vs Big Data.

UNIT II: **(9 Lectures)**

Hadoop Architecture and HDFS: What is Hadoop? Hadoop History, Distributing Processing System, Core Components of Hadoop, HDFS Architecture, Hadoop Master – Slave Architecture, Daemon Types, Name node, Data node, Secondary Name node.

Hadoop Clusters and the Hadoop Ecosystem- What is Hadoop Cluster? Pseudo Distributed mode, Type of Clusters, Hadoop Ecosystem: Pig, Hive, Flume, SQOOP.

UNIT III: **(10 Lectures)**

Hadoop MapReduce Framework: Overview of MapReduce Framework, MapReduce Architecture, Job Tracker and Task Tracker, Use Cases of Map Reduce, Anatomy of Map Reduce Program.

MapReduce Programs in Java: Basic MapReduce API Concepts, Writing MapReduce Driver, Mappers, and Reducers in Java, Speeding up Hadoop Development by Using Eclipse, Word Count Example and Weather Dataset Example.

UNIT IV: **(12 Lectures)**

Hive and HiveQL- What is Hive? Hive vs MapReduce, Hive DDL : Create/Show/Drop Tables, Internal and External Tables, Hive DML : Load Files & Insert Data, Hive Architecture & Components, Difference between Hive and RDBMS, Partitions in Hive.

Pig: Pig vs MapReduce, Pig Architecture & Data types, Shell and Utility components, Pig Latin Relational Operators, Pig Latin: File Loaders and UDF, Programming structure in UDF, Pig Jars Import and limitations of Pig.

UNIT V: (9 Lectures)

Apache SQOOP: Why and What is SQOOP?, SQOOP Architecture, Benefits of SQOOP, Importing Data Using SQOOP.

Apache Flume: Introduction, Flume Model and Goals, Features of Flume, Flume Use Cases.

Course Outcomes:

Upon completion of this course, the students will be able to:

CO 1. Outline importance of Big Data in solving real time problems in data analytics.

CO 2. Illustrate Hadoop ecosystem and its components in detail.

CO 3. Make use of distributed file systems and Hadoop and can write MapReduce programs to solve complex problems.

CO 4. Explore the Hadoop ecosystems core components and apply in real-time scenarios.

Mapping of COs to POs:

POs/ COs	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2
CO1	3	3	3	3	3	-	-	-	-	-	-	-	3	3
CO2	3	3	3	3	3	-	-	-	-	-	-	-	3	3
CO3	3	3	3	3	3	-	-	-	-	-	-	-	3	3
CO4	3	3	3	3	3	-	-	-	-	-	-	-	3	3

TEXT BOOKS:

1. Tom White, Hadoop : The Definitive Guide, 3rd Edition, O’reilly
2. Dirk deRoos, Chris Eaton, George Lapis, Paul Zikopoulos, Tom Deutsch, “Understanding Big Data Analytics for Enterprise Class Hadoop and Streaming Data”, 1st Edition, TMH.

REFERENCE BOOKS:

1. Alex Holmes, Hadoop in Practice, MANNING Publications.
2. Srinath Perera, Thilina Gunarathne, Hadoop MapReduce Cookbook, Packt publishing.

DART PROGRAMMING
(JOB ORIENTED ELECTIVE-I)

	L	T	P	C
Subject Code: UGCS7T0222	**L**	**T**	**P**	**C**
IV Year / I Semester	**2**	**0**	**2**	**3**

Prerequisites:

- Basic Understanding of programming concepts.
- Familiarity with a programming languages like C, Java and Python

Course Objectives:

This course is designed to introduce engineering students to the Dart programming language, which is widely used for web and mobile application development. Students will learn the core concepts of Dart, gain hands-on experience in building Dart applications, and explore how Dart can be used in engineering-related projects.

Syllabus:

UNIT I: Introduction to Dart (9 Hours)

Overview of Dart and its history, Features, Setting up the development environment (IDEs and editors), Hello World in Dart, Identifiers, Keywords, Comments, Variables, data types, dynamic type and operators, final and const.

UNIT II: Control Flow and Functions (9 Hours)

Conditional statements (if, if else, else if ladder, switch), Loops (for, while, do-while), Control Statements (break, Continue) Functions and parameter passing, Optional Parameters, Recursive Dart function, Lambda function, Scope and lifetime of variables

UNIT III: Collections and Error Handling (12 Hours)

Lists: Fixed length & Growable Lists, Properties, Operations, Sets: Different ways of declaring, adding elements into set, Operations, Functions, Converting Set to List in Dart.

Maps: Different ways of declaring a Map, Properties and Functions, Converting Set to Map in Dart, Iterating through collections, **Exception handling**: try / on / catch Blocks, Custom Exceptions.

UNIT IV: Object-Oriented Programming in Dart (9 Hours)

Classes and objects, Constructors, super Constructor, this, static, and super keywords, methods & method overriding , Inheritance and polymorphism, getters & setters, Abstract classes and interfaces

UNIT V: Dart for Web Development, Flutter (10 Hours)

Dart for Web Development: Introduction to web development with Dart, Building web applications using HTML and Dart, Handling user input and events.

Introduction to Flutter: Overview of Flutter and its role in mobile app development, creating a simple mobile app with Flutter and Dart, Introduction to Widgets and layouts in Flutter.

Course Outcomes:

Upon completion of the course, the students will be able to:

CO 1 : Understand the Dart syntax, semantics, basic programming constructs to be used to write the programs. [L2]

CO 2 : Utilize the methods of various data structures / Collections to manipulate the data. [L3]

CO 3 : Apply the appropriate Object-Oriented Programming principle for a given scenario. [L3]

CO 4 : Develop bug free applications by handling different types of exceptions. [L4]

CO 5 : Understand the how to use the dart in web development and Flutter. [L2]

Mapping of COs to POs:

POs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO 10	PO 11	PO 12	PSO 1	PSO 2
CO1	2	-	-	-	-	-	-	-	-	-	-	-	-	-
CO2	2	-	-	-	-	-	-	-	-	-	-	-	-	-
CO3	-	-	-	-	3	-	-	-	-	-	-	-	-	-
CO4	-	-	3	-	-	-	-	-	-	-	-	-	2	-
CO5	-	-	-	-	3	-	-	-	-	-	-	-	-	-

TEXT BOOKS:

1. "Dart Up and Running" by Kathy Walrath and Seth Ladd
2. "Dart: Scalable Application Development" by Luca Zampetti and Vincenzo Gianferrari Pini

ONLINE RESOURCES:

1. Dart Official Website: www.dart.dev
2. DartPad: www.dartpad.dev
3. Flutter Documentation: www.docs.flutter.dev

DEVOPS
(JOB ORIENTED ELECTIVE-I)

Subject Code: UGCS7T0422	**L**	**T**	**P**	**C**
IV Year / I Semester	**2**	**0**	**2**	**3**

Prerequisites: Good exposure to Software Engineering concepts and Software Development Methodologies.

Course Objectives:
To get an expertise on the culture of DevOps in Software Development Methodologies for finding ways to adapt and innovate social structure, culture and technology together in order to work more effectively in the Enterprises.

Syllabus:

UNIT I: **(8 Lectures)**
Introduction to DevOps: What is DevOps, A History of DevOps, Fundamental Terminology and Concepts – Software Development Methodologies, Operations Methodologies, Systems Methodologies, Development Release and Deployment Concepts, Infrastructure Concepts, Cultural Concepts. DevOps Misconceptions and Anti-Patterns, the Four Pillars of Effective DevOps.

UNIT II: **(8 Lectures)**
Collaboration: Defining Collaboration, Individual Differences and Backgrounds, Opportunities for Competitive Advantage, Mentorship, Introducing Mindsets, Mindsets and Learning Organizations, The Role of Feedback, Reviews and Rankings, Communication and Conflict Resolution Styles, Empathy and Trust, Humane Staffing and Resources, Misconceptions and Troubleshooting of Collaboration.

UNIT III: **(12 Lectures)**
Affinity: What Makes a Team, Teams and Organizational Structure, Finding Common Ground Between Teams, Benefits of Improved Affinity, Requirements for Affinity, Measuring Affinity, Misconceptions and Troubleshooting of Affinity.

Tools: Software Development, Automation, Monitoring, Evolution of the Ecosystem,The Value of Tools to People, What Are Tools?, The Right Tools for Real Problems, Embracing Open Source, Standardization of Tools, Consistent Processes for Tool Analysis, Exceptions to Standardization, Irrelevance of Tools, The Impacts of Tools on Culture, Selection of Tools, Auditing Your Tool Ecosystem, Elimination of Tools, Misconceptions and Troubleshooting of Tools.

UNIT IV: **(8 Lectures)**

Scaling: Understanding Scaling, Considering Enterprise DevOps, Organizational Structure, Team Flexibility, Organizational Lifecycle, Complexity and Change, Scaling for Teams, Team Scaling and Growth Strategies, Scaling for Organizations, Misconceptions and Troubleshooting of Scaling.

UNIT V: **(6 Lectures)**

DevOps Practices: Implementing CI/CD and continuous deployment, Understanding IaC practices, DevOps Best Practices: Automating everything, Choosing the right tool,Writing all your configuration in code, Designing the system architecture, Building a good CI/CD pipeline, Integrating tests, Applying security with DevSecOps, Monitoring your system, Evolving project management.

Course Outcomes:

Upon completion of this course, the students will be able to:

CO 1. Make use the Influence of DevOps on Software Development Methodologies along with its Misconceptions and Anti-Patterns.

CO 2. Illustrate the Methodologies of Four Pillars of DevOps and Troubleshoot the common problems that can arise in the effective DevOps.

CO 3. Inference the culture of DevOps to the Enterprises for achieving agility and innovation in its business units.

Mapping of COs to POs:

POs/ COs	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2
CO1	3	3	-	-	-	-	-	-	-	-	3	-	-	-
CO2	3	3	3	3	-	-	-	-	-	-	3	-	-	-
CO3	3	3	3	3	-	-	-	-	-	-	3	-	-	-

TEXT BOOKS:

1. Jennifer Davis, RynDaniels, Effective DevOps: Building a Culture of Collaboration, Affinity, and Tooling at Scale, O'Reilly.
2. Mikael Krief, Learning DevOps, Packt Publications.

REFERENCE BOOKS:

1. Verona, Joakim. Practical DevOps. Packt Publishing Ltd.
2. By Jez Humble and David Farley, Continuous Delivery: Reliable Software Releases through Build, Test and Deployment Automation, Addison-Wesley Professional
3. Mandi Walls,Building a DevOps Culture, O'Reilly publications.
4. Sanjeev Sharma, "The DevOps Adoption Playbook – A Guide to Adopting DevOps in a Multi-Speed IT Enterprise", Wiley Publications.

BLOCKCHAIN TECHNOLOGIES
(JOB ORIENTED ELECTIVE-II)

	L	T	P	C
Subject Code: UGCS7T1722	**L**	**T**	**P**	**C**
IV Year / I Semester	**2**	**0**	**2**	**3**

Prerequisites: Familiarity with Information Security and Computer Networks.

Course Objectives: This course introduces the fundamentals and implementation issues of Blockchain Technologies.

Syllabus:

UNIT I: **(8 Lectures)**

Grasping Blockchain Fundamentals

Tracing Blockchain's Origin, The shortcomings of current transaction systems,The emergence of bitcoin,The birth of blockchain,Revolutionizing the Traditional Business Network,Exploring a blockchain application, Recognizing the key business benefits, Building trust with blockchain.

UNIT II: **(8 Lectures)**

Taking a Look at How Blockchain Works

Why It's Called "Blockchain", What Makes a Blockchain Suitable for Business?, Shared ledger, Permissions, Consensus, Smart contracts ,Identifying Participants and Their Roles.

UNIT III: **(12 Lectures)**

Propelling Business with Blockchains

Recognizing Types of Market Friction, Information frictions, Interaction frictions, Innovation frictions, Moving Closer to Friction-Free Business Networks, Reducing information friction, Easing interaction friction, Easing innovation friction, Transforming Ecosystems through Increased Visibility.

Blockchain in Action: Use Cases

Financial Services,Commercial financing,Trade finance,Cross-border transactions, Insurance, Government, Supply Chain Management, Healthcare, Electronic medical records Healthcare payments pre-authorization, Internet of Things(IoT).

UNIT IV: **(8 Lectures)**

Hyperledger, a Linux Foundation Project

Hyperledger Vision, Hyperledger Fabric, How Can IBM Help Developers Innovate With Blockchain? Offering an easily accessible cloud and development platform, Individualized attention and industry expertise.

UNIT V: (8 Lectures)

Problems with Block chain

Security and Safeguards, Protection from attackers, Hacks on exchanges, What is stopping adoption?, Scalability problems, Network attacks to destroy bitcoin, Case Study: Failed currencies & blockchain.

Course Outcomes:

Upon completion of this course, the students will be able to:

CO 1. Infer and summarize the fundamentals of Blockchain.

CO 2. Analyze the working of Blockchain.

CO 3. Explain how business can be easily made with Blockchain.

CO 4. Interpret how Blockchain can be integrated with various current technologies.

CO 5. Examine and test the Blockchain strength in providing solutions.

CO 6. Investigate and understand the Problems with Blockchain.

Mapping of COs to POs:

POs/ COs	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2
CO1	3	3	-	-	-	-	-	-	-	-	-	-	-	-
CO2	3	2	3	3	-	-	-	-	-	-	-	-	-	-
CO3	3	3	3	3	-	-	-	-	-	-	-	3	-	-
CO4	3	2	3	3	-	-	-	-	-	3	-	3	-	-
CO5	3	3	3	3	2	-	-	-	-	-	-	3	-	3
CO6	3	3	3	3	3	-	-	-	-	-	-	3	-	3

TEXT BOOKS:

1. Manav Gupta, Blockchain for Dummies, IBM Limited Edition, John Wiley & Sons.

REFERENCE BOOKS:

1. Swan, Melanie. Blockchain: Blueprint for a new economy. O'Reilly Media, Inc.

ARTIFICIAL INTELLIGENCE
(JOB ORIENTED ELECTIVE-II)

	L	T	P	C
Subject Code: UGCS7T0822	**L**	**T**	**P**	**C**
IV Year / I Semester	**2**	**0**	**2**	**3**

Prerequisites: Familiarity with Discrete Mathematics, Linear Algebra and Probability.

Course Objectives: The objective of the course is to present an overview of artificial intelligence principles and approaches.

Syllabus:

UNIT I: **(8 Lectures)**
Introduction to artificial intelligence: Introduction, history, intelligent systems, foundations of AI, applications, tic-tac-toe game playing, development of AI languages, current trends in AI. **Problem solving: state-space search and control strategies:** Introduction, general problem solving, characteristics of problem.

UNIT II: **(7 Lectures)**
Search Strategies: exhaustive searches, heuristic search techniques, a*, constraint satisfaction.

UNIT III: **(12 Lectures)**
Logic concepts: Introduction, propositional calculus, proportional logic, natural deduction system, axiomatic system, semantic tableau system in proportional logic, resolution refutation in proportional logic, predicate logic.

Knowledge representation: Introduction, approaches to knowledge representation, knowledge representation using semantic network, extended semantic networks for KR, knowledge representation using frames.

UNIT IV: **(9 Lectures)**
Advanced knowledge representation techniques: Introduction, conceptual dependency theory, script structure, cyc theory.
Expert system and applications: Introduction phases in building expert systems, expert system versus traditional systems, rule-based expert systems blackboard systems truth maintenance systems, application of expert systems, list of shells and tools.

UNIT V: **(8 Lectures)**

Uncertainty measure: probability theory: Introduction, probability theory, Bayesian belief networks, certainty factor theory, dempster-shafer theory.

Course Outcomes:

Upon completion of this course, the students will be able to:

CO 1 Summarize and formulate appropriate logic concepts and AI methods for solving a problem.

CO 2 Applying various searching, game playing, and knowledge representation techniques to solve the real world problems.

CO 3 Analyze different expert systems and its applications.

CO 4 Explain the concepts of probability theory, fuzzy sets and fuzzy logic for uncertainty measure.

Mapping of COs to POs:

POs/ COs	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2
CO1	3	-	-	-	-	-	-	-	-	-	-	-	-	-
CO2	3	3	3	-	-	-	-	-	-	-	-	-	-	-
CO3	3	3	-	-	-	-	-	-	-	-	-	-	-	-
CO4	3	-	-	-	-	-	-	-	-	-	-	-	-	-

TEXT BOOKS:

1. Saroj Kaushik, Artificial Intelligence, CENGAGE Learning.
2. Stuart Russel, Peter Norvig, Artificial intelligence, A modern Approach, 2nd ed, PEA.
3. Rich, Kevin Knight, Shiv Shankar B Nair, Artificial Intelligence, 3rd ed, TMH.
4. Patterson, Introduction to Artificial Intelligence, PHI.

REFERENCE BOOKS:

1. George F Lugar ,Artificial intelligence, structures and Strategies for Complex problem solving, 5th ed, PEA.
2. Ertel, Wolf Gang, Introduction to Artificial Intelligence, Springer.
3. Nils J Nilsson, A new Synthesis Artificial Intelligence, Elsevier.

GO PROGRAMMING
(JOB ORIENTED ELECTIVE-II)

	L	T	P	C
Subject Code: UGCS7T1922	**L**	**T**	**P**	**C**
IV Year / I Semester	**2**	**0**	**2**	**3**

Prerequisites: Familiarity with any programming language.

Course Objectives:
The course is designed to cover the basics and then dive into more advanced features of the Go programming language.

Syllabus:

UNIT I: (7 Lectures)
Introduction: Origins and evolution, Languages that influenced Go, Why a new language?, Targets of the language, Guiding design principles, Characteristics of the language, Uses of the language, Missing features, Programming in Go.
Program Structure: Names, Declarations, Variables, Assignments, Type Declarations, Packages and Files, Scope.

UNIT II: (9 Lectures)
Basic Data Types: Integers, Floating-Point Numbers, Complex Numbers, Booleans, Strings, Constants.
Control Structures: if else construct, switch construct, for construct, break, continue and labels.
Composite Types: Arrays, Slices, Maps, Structs, JSON,Text and HTML Templates.

UNIT III: (12 Lectures)
Functions: Function Declarations, Recursion, Multiple Return Values, Errors, Function Values, Anonymous Functions, Variadic Functions, Deferred Function Calls, Panic, Recover.
Methods: Method Declarations, Methods with a Pointer Receiver, Composing Types by Struct Embedding, Method Values and Expressions, Encapsulation.

Interfaces: Interfaces as Contracts, Interface Types, Interface Satisfaction, Parsing Flags with flag.Value, Interface Values, The error Interface, Type Assertions, Discriminating Errors with Type Assertions, Querying Behaviors with Interface Type Assertions, Type Switches.

UNIT IV: (12 Lectures)
Reading and Writing: Reading input from the user, Reading from and writing to a

file, Copying files, Reading arguments from the command-line, Reading files with a buffer, Reading and writing files with slices, Using defer to close a file.

Goroutines and Channels: Goroutines, Concurrent Clock Server, Concurrent Echo Server, Channels, Looping in Parallel, Concurrent Web Crawler, Multiplexing with select, Concurrent Directory Traversal, Cancellation, Chat Server.

Concurrency with Shared Variables: Race Conditions, Mutual Exclusion, Read/Write Mutexes, Memory Synchronization, Lazy Initialization, The Race Detector, Concurrent Non Blocking Cache, Goroutines and Threads.

UNIT V: (8 Lectures)

Packages and Go Tool: Introduction, Import Paths, The Package Declaration, Import Declarations, Blank Imports, Packages and Naming, The Go Tool.

Testing: Go Test Tool, Test Functions, Coverage, Benchmark Functions, Profiling, Example Functions.

Course Outcomes:

Upon completion of this course, the students will be able to:

CO 1. Study the basic constructs of Go Programming and learn its structural elements in detail.

CO 2. Develop modular programming and make use of functions and methods.

CO 3. Implement the Interfaces and Goroutines for executing the program independently and simultaneously.

CO 4. Perform Testing and apply concurrency in Go programs and examine different packages in Go.

Mapping of COs to POs:

POs/ COs	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2
CO1	3	3	-	-	-	-	-	-	-	-	-	-	3	-
CO2	3	3	3	3	-	-	-	-	-	-	-	-	3	-
CO3	3	3	3	3	-	-	-	-	-	-	-	-	3	-
CO4	3	3	3	3	-	-	-	-	-	-	-	-	3	-

TEXT BOOKS:

1. Alan A. A. Donovan, Brian W. Kernighan, "The Go Programming Language", Addison-Wesley.
2. Ivo Balbaert, "The Way to GO – A Thorough Introduction to the Go Programming Language", i-Universe Publisher.

REFERENCE BOOKS:

1. Mark Summerfield, Programming in Go: Creating applications for the 21st century. Addison-Wesley.

2. Caleb Doxsey, An Introduction to Programming in Go.
3. Tarik Guney, “Hands-On Go Programming: Explore Go by solving real-world challenges”, Packt Publishing.
4. John P. Baugh, “Go Programming”, CreateSpace Publisher.
5. Mat Ryer, Go Programming Blueprints, Packt Publishing.

ROBOTIC PROCESS AUTOMATION
(JOB ORIENTED ELECTIVE-II)

Subject Code: UGCS7T2022	L	T	P	C
IV Year / I Semester	2	0	2	3

Prerequisites: A little bit of C programming knowledge, analytical and logical thought procedure to build a process is required.

Course Objectives: This course will give you an overview of robotic process automation (RPA) technology. You will learn the characteristics, benefits, risks, and challenges of RPA. You will learn about the RPA landscape, how RPA is transforming businesses and how it is affecting accounting and finance professionals.

Syllabus:

UNIT I: (7 Lectures)

RPA Foundations: RPA, Flavors of RPA, History of RPA, Benefits of RPA, Downsides of RPA, RPA Compared to BPO, BPM, and BPA; Consumer Willingness for Automation, Workforce of the Future and RPA Skills.

UNIT II: (8 Lectures)

Planning: RPA Consulting: Some Case Studies, What to Automate? ROI for RPA, RPA Use Cases, The Plan and RPA Vendor Evaluation.

Center of Excellence: CoE, Need of CoE, Forming the Team, Business Analyst, Developer, RPA Solution Architect, RPA Supervisor, What Should a CoE Do?, Communication, Change Management.

UNIT III: (12 Lectures)

Bot Development: Installation of UiPath, Activities, Flowcharts and Sequences, Log Message, Variables, Loops and Conditionals, Switch, Debug, Common UiPath Functions, The UiPath Orchestrator, Best Practices.

Deployment and Monitoring : Testing, Going into Production, Monitoring, Security, Scaling.

Data Preparation: Types of Data, Big Data, Issues with Big Data, Data Process, Types of Algorithms, Bias and Open Source RPA.

Using Blue Prism: Building the first Blue Prism process, Pages, Data Items, Blocks, Collections, Loops, Actions, Decisions, Choices and Calculations.

UNIT IV: (10 Lectures)

Implementing Business Objects: Creating a business object, Business Studio, Renaming actions, Application Modeller, Using the Navigate stage, Publishing an action, Using a custom Business Object from a process.

Spying Elements: Spying elements on a web page, How does spying work?, Tweaking and Tightening the match criteria, Adding and Categorizing elements, More spy modes, UI Automation mode, UI Automation navigator, Surface automation with region mode.

Write, Wait, and Read: Creating the search action, Writing to text boxes, Clicking buttons, Wait stage, Read stage, Reading the search results, Using dynamic match attributes.

UNIT V: (10 Lectures)

Excel & Email Automation: Reading the shopping list, Importing the Excel VBO, Using MS Excel VBO, Opening an Excel file, Reading an entire worksheet into a collection, Writing to a cell, Considerations for CSV, Sending and Receiving Emails.

Control Room and Work Queue: Publishing a process, Running a process, Scheduling processes and work queues.

Exception Handling: Expected and unexpected exceptions, Raising exceptions, Handling exceptions, Debugging and troubleshooting from the control room.

Course Outcomes:

Upon completion of this course, the students will be able to:

CO1. Understand the different RPA tools and its architecture for process development.

CO2. Acquire the basic knowledge on UiPath and Blue Prism softwares.

CO3. Apply the different stages to create and demonstrate static processes.

CO4. Demonstrate the Blue Prism business studio and its stages by creating real time applications.

CO5. Classify the exception handling and error management techniques with different stages in RPA.

Mapping of COs to POs:

PO/ CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	3	3	3	-	-	-	2	-	2	3	-
CO2	3	3	3	3	2	3	-	-	-	2	-	3	2	-
CO3	2	2	3	2	3	3	-	-	-	2	-	3	3	-
CO4	2	3	3	3	3	3	-	-	-	2	-	2	2	-
CO5	3	3	3	3	3	3	-	-	-	2	-	2	3	-

TEXT BOOKS:

1. Tom Taulli, The Robotic Process Automation Handbook: A Guide to Implementing RPA Systems, Apress.

2. Lim Mei Ying, Robotic Process Automation with Blue Prism Quick Start Guide, Packt Publishing.

REFERENCE BOOKS:

1. Alok Mani Tripathi, Learning Robotic Process Automation, Packt Publishing Ltd.
2. Kelly Wibbenmeyer, The Simple Implementation Guide to Robotic Process Automation (RPA): How to Best Implement RPA in an Organization, iUniverse.

MANAGEMENT SCIENCE
(Common to all branches)

Subject Code : UGMB7T0122	**L**	**T**	**P**	**C**
IV Year / I Semester	**3**	**0**	**0**	**3**

Prerequisites:

- General awareness about Principles of Management.
- To have an insight about Production and Operations Management.
- To be able to acquire knowledge about Human Resource Management, Marketing, Strategic Management.

Course Objectives:

1. To create awareness about different Managerial concepts like Management, Production, Marketing, Human Resource and Strategic Management.
2. To make the students equip with knowledge on techniques of PERT and CPM in project management.

Syllabus:

UNIT-I: [8 Hrs]

Introduction to Management : Concept and importance of Management, Functions of management, Evaluation of Management thought, Fayol's principles of Management, Maslow's need hierarchy & Herzberg's two factor theory of Motivation, Decision making process, Designing organizational structure, Principles of Organization, Types of organization structures.

UNIT-II: [8 Hrs]

Operations Management : Plant Location Principles and types of plant Layout , Work study, Materials Management: Objectives - Need for inventory control-Inventory control techniques EOQ , ABC, HML, SDE, VED and FSN analysis.

UNIT-III: [12 Hrs]

Human Resources Management (HRM): Concepts of HRM, Basic functions of HR manager, Job Evaluation and Merit Rating, Performance Appraisal, Methods of Performance appraisal Concepts Compensation.

Marketing Management: Functions of marketing, Marketing Mix, Marketing strategies based on Product life cycle, Channels of distribution (Place), Promotional Mix.

UNIT-IV: [10 Hrs]

Project Management (PERT/CPM): Network analysis, Program Evaluation and

Review Technique (PERT), Critical path method (CPM) - Identifying critical path, Difference between PERT & CPM (simple problems).

UNIT-V: **[8 Hrs]**

Strategic Management: Mission, Goals, objectives, policy, strategy, Environmental scanning, SWOT analysis, Steps in strategy formulation and implementation Generic strategy alternatives.

Course Outcomes:

Upon completing the course, student will be able to

COs	Description	Blooms Level
CO 1	Understand the fundamentals of Management with specific insight as its function and role	Understanding
CO 2	Learn the concepts of production, Management of human Resources and Management of Marketing activities along with business environment	Understanding
CO 3	Apply the problem solving skills to demonstrate logical solution to real life problems	Applying
CO 4	Create the awareness of business strategies to deal with the dynamic business environment	Creating

Mapping of COs to POs:

POs	1	2	3	4	5	6	7	8	9	10	11	12	PSO 1	PSO 2
CO 1	-	-	-	-	-	-	-	-	2	-	-	-	-	-
CO 2	-	-	-	-	-	2	-	-	-	-	-	-	-	-
CO 3	-	-	-	-	-	-	-	-	-	-	2	-	-	-
CO 4	-	-	-	-	-	-	-	-	-	-	2	-	-	-

Text Books:

T1. Dr. Arya Sri, "Management Science", TMH 2011.

T2. L.M. Prasad, "Principles & Practices of Management" Sultan chand & Sons, 2007.

Reference Books:

R1. K. Aswathappa and K. Sridhara Bhat, "Production and Operations Management", Himalaya Publishing House, 2010.

R2. Philip Kotler Philip Kotler, Kevin Keller, Mairead Brady, Malcolm Goodman, Torben Hansen, "Marketing Management" Pearson Education Limited, 2016.

AMAZON WEB SERVICES
(Skill Oriented Course)

	L	T	P	C
Subject Code: UGCS7K2122	**L**	**T**	**P**	**C**
IV Year / I Semester	**1**	**0**	**2**	**2**

Prerequisites: Familiarity with basics of cloud computing.

Course Objective: The objective of this course is to get the skills pertaining to Amazon Web services.

Syllabus:

AWS Compute Services: Amazon Elastic Compute Cloud, Different types of instances in Amazon Web Services- General purpose instances, Compute Optimized instances, Memory Optimized instances, Accelerated Computing instances, Storage Optimized instances.

AWS Storage Services: Different types of AWS Storage Services, Amazon Simple Storage Service, Amazon Elastic Block storage, Amazon Glacier storage service.

AWS Database Services: Types of Database services in AWS environment - Relational and Key value types- Amazon DynamoDB.

AWS Security: AWS Security Groups, AWS Virtual Private Cloud.

Experiments:

1. Launch an EC2 instance in AWS environment using a general purpose instance (either in Windows environment or Linux environment).
2. Create a sample web application which runs in AWS to store the data by using AWS S3 service.
3. Launch an EC2 Linux instance in AWS environment then attach and mount EBS volume to EC2 instance.
4. Launch an AWS DynamoDB instance which supports the type i.e. key value pair databases (Unstructured data)
5. Create a Virtual Private Cloud in Amazon Web Services and launch an EC2 instance of your own choice i.e. either Linux or windows instance

Course Outcomes:

Upon completion of this course, the students will be able to:
CO1 Deploy virtual instances on AWS platform using Amazon EC2 Service.
CO2 Demonstration of storage services on AWS platform.
CO3 Deployment of Database instances on AWS platform.
CO4 Apply security on AWS platform.

Mapping of COs to POs:

POs/ COs	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2
CO1	3	-	3	-	3	-	-	-	2	-	-	-	-	3
CO2	3	-	3	-	3	-	-	-	-	-	-	-	-	3
CO3	3	-	3	-	3	-	-	-	-	-	-	-	-	3
CO4	3	2	3	-	3	-	-	-	-	-	-	-	-	3

Text Books:

1. Mark Wilkins, Learning Amazon Web Services (AWS): A Hands-On Guide to the Fundamentals of AWS Cloud, Pearson Education.
2. Bernard Golden, Amazon Web Services for Dummies, John Wiley & Sons.

Reference Books:

1. Andreas Wittig & Michael Wittig, Amazon Web Services in Action, Manning Publications.
2. Aurobindo Sarkar, Amit Shah, Learning AWS, Packt Publishing.
3. Richard Derry, Amazon Web Services: The Complete Guide From Beginners For Amazon Web Services,
4. Joe Baron, Hisham Baz, Tim Bixler, AWS Certified Solutions Architect Official Study Guide, Wiley
5. Bert David, Amazon Web Services Tutorial for Beginners, Lightning Source
6. George Sammons, Introduction to AWS Beginner's Guide Book
7. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html
8.https://docs.aws.amazon.com/whitepapers/latest/aws-overview/storage-services.html
9. https://docs.aws.amazon.com/whitepapers/latest/aws-overview/database.html
10. https://docs.aws.amazon.com/lex/

GAME DEVELOPMENT
(Skill Oriented Course)

	L	T	P	C
Subject Code: UGCS7K2222	**L**	**T**	**P**	**C**
IV Year / I Semester	**1**	**0**	**2**	**2**

Prerequisites: HTML, Java Script and Animation Techniques.

Course Objectives: Understanding the processes, mechanics and issues in game design and development. At the end, the student will be in a position to create interactive games.

Syllabus:

UNIT I: Creating a Basic Game World (6 Lectures)
A Basic HTML Page, Canvas Element, Audio Element, Image Element, Animation: Timer and Game Loops. Basic HTML Layout, Creating the Splash Screen and Main Menu, Level Selection, Loading Images, Loading Levels, Animating the Game, Handling Mouse Input, Defining Our Game States.

UNIT II: Game Engine Basics (6 Lectures)
Box2D Fundamentals, Adding More Box2D Elements, Tracking Collisions and Damage, Drawing Our Own Characters, Defining Entities, Adding Box2D, Creating Entities, Adding Entities to Levels, Setting Up Box2D Debug Drawing, Drawing the Entities, Animating the Box2D World, Adding Sound.

UNIT III: Creating a Mobile Game (4 Lectures)
Challenges in Developing for Mobile Devices, Making the Game Responsive, Fixing Mouse and Touch Event Handling, Loading the Game on a Mobile Device, Fixing Audio Problems on Mobile Browsers, Adding Some Finishing Touches.

UNIT IV: Creating the Real-time strategy(RTS) Game World (6 Lectures)
Basic HTML Layout, Creating the Splash Screen and Main Menu, Creating Our First Level, Loading the Mission Briefing Screen, Implementing the Game Interface, Implementing Map Panning.

Adding Entities to Our World
Defining Entities, Adding Entities to the Level, Drawing the Entities, Adding the required features, Selecting Game Entities, Highlighting Selected Entities.

UNIT V: Intelligent Unit Movement (6 Lectures)
Commanding Units, Sending and Receiving Commands, Processing Orders, Implementing Aircraft Movement, Pathfinding, Defining Our Pathfinding Grid, Implementing Vehicle Movement, Collision Detection and Steering, Deploying the

Harvester, Smoother Unit Movement, Customizing Your Code Editor, Writing Modular Code, Automating Development Workflow.

Course Outcomes:

Upon completion of this course, the students will be able to:
CO1: Create a basic game world and understand the game engine basics.
CO2: Develop mobile games and real-time strategies for games.
CO3: Add entities to game world and apply movements.

Mapping of COs to POs:

POs/ COs	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2
CO1	3	3	3	-	3	-	-	-	3	-	-	3	3	-
CO2	3	3	3	-	3	-	-	3	3	-	-	-	3	-
CO3	3	3	3	-	3	-	-	3	3	-	-	-	3	-

TEXT BOOKS:

1. Aditya Ravi Shankar, "Pro HTML5 Games Learn to Build your Own Games using HTML5 and JavaScript", Apress
2. Graeme Stuart, "Introducing JavaScript Game Development", Apress

REFERENCE BOOKS:

1. Mike Geig, " Unity Game Development", Pearson Publishers
2. Michelle Menard and Bryan Wagstaff, "Game Development with Unity", Cengage Learning.
3. Joseph Hocking, "Unity in Action(Multiplatform game development in C#)", Manning Publications.
4. Will McGugan, "Beginning Game Development with Python and Pygame", Apress
5. Sloan Kelly, "Python, PyGame and Raspberry Pi Game Development", Apress
6. Al Sweigart, "Invent your own computer games with python", No Starch Press
7. Jonathan S. Harbour, "Beginning Game Programming", Cengage Learning
8. CAROL VORDERMAN MBE, "Coding Games in Python", DK Publishing

DATA VISUALIZATION
(Skill Oriented Course)

	L	T	P	C
Subject Code: UGCS7K3822				
IV Year / I Semester	**1**	**0**	**2**	**2**

PREREQUISITES:

Familiarity in Python programming.

COURSE OBJECTIVE:

The objective is to expose the students to the various key aspects of data visualization tools and technologies because data visualization is essential to analyze massive amounts of information and make data-driven decisions. This lab uses the desirable and unique features tableau or python for data visualization tool because of ease in tableau tool interface or python graphical packages. Their powerful data discovery and exploration application allows users to answer important questions in seconds and solutions for all kinds of industries, departments and data environments.

LIST OF EXPERIMENTS:

1. Tableau overview, environment setup, navigation and data types,
2. Introduction to usage of python 3 packages - matplotlib, numpy, pandas, seaborn, ggplot, ggplot2, plotly
3. Demonstrate the usage of data sources, custom data view and extracting data fields operations
4. Experimenting with data editing, metadata, data joining and data blending
5. Implementation of calculations with operators functions, and numeric calculations
6. Implementation of calculations with operations on string, date and table
7. Experiment to working with sorting and filtering operations
8. Experiment to demonstrate data visualization with charts: bar chart, line chart and pie chart
9. Experiment to demonstrate data visualization with charts: crosstab, scatter plot and bubble chart
10. Experiment to demonstrate data visualization with charts: bullet graph, box plot and tree map/heat map
11. Experiment to demonstrate data visualization with charts: bump chart, gantt chart and histograms
12. Experiment to demonstrate data visualization with charts: motion charts and waterfall charts
13. Experiment to demonstrate building a dashboard with tables and charts for any business applications
14. Experiment to demonstrate data visualization for prediction and forecasting with trend lines
15. Construction of advanced visualization with waffle charts.
16. Construction of advanced visualization with word clouds
17. Construction of advanced visualization sea born and regression plots
18. Creating maps and visualizing geospatial data with folium and map styles

19. Creating maps and visualizing geospatial data using maps with markers
20. Creating maps and visualizing geospatial data using choropleth maps

COURSE OUTCOMES:

Upon the successful completion of the course, the student will be able:

CO1: Design features to use many visual components.

CO2: Apply and analyze best practices in data visualization to develop charts, tables, maps, and other visual representations of data.

CO3: Plan interactive dashboards to combine several visualizations into a single unit for effective communication.

CO4: Evaluate data with advanced visualizations techniques and by exploring visualization on geospatial data.

MAPPING OF COs TO POs:

POs/ COs	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2
CO1	3	3	3	3	3	-	-	-	-	-	-	-	-	-
CO2	3	3	3	3	3	-	-	-	-	-	-	-	-	3
CO3	3	3	3	3	3	-	-	3	-	3	3	-	3	3
CO4	3	3	3	3	3	-	-	-	-	-	-	-	-	3

TEXT BOOKS:

1. Joshua N Milligan, Learning Tableau 2019 Tools for Business Intelligence, data prep, and visual analytics, 3e,Packt publications.
2. Wes McKinney, Python for Data Analysis, ie, O'Reilly.
3. Fabio Nelli, Python Data Analytics With Pandas, NumPy, and Matplotlib, 2e, A Press.
4. Ryan Sleeper, Practical Tableau 100 TIPS, TUTORIALS, AND STRATEGIES FROM A TABLEAU, 1e, O’Reilly.
5. Ashutosh Nandeshwar, Tableau Data Visualization Cookbook, 1e, Packt Publishing.

REFERENCE BOOKS:

1. Daniel G. Murray, Tableau your data, 1e, Wiley.
2. Fabio Nelli, Python Data Analytics, 1e, A Press.
3. Ben Jones, Communicating Data with Tableau,1e, O’Reilly.

Web Links:

1. https://www.tableau.com/academic/students
2. https://www.tableau.com/learn/articles/data-visualization

BUG BOUNTY HUNTING
(Skill Oriented Course)

	L	T	P	C
Subject Code: UGCS7K3922	**L**	**T**	**P**	**C**
IV Year / I Semester	**1**	**0**	**2**	**2**

Prerequisites: Knowledge of programming, Web development and Networking Concepts.

Course Objectives:

This course introduces students to the principles and practices of identifying and responsibly disclosing security vulnerabilities in software and web applications. It covers both theoretical concepts and practical hands-on exercises.

Syllabus:

Introduction to Hunting: Bug Bounty Platforms, Introducing Burp Suite, OWASP ZAP and Web Goat, Setting Up Your Environment, Why We Need a Virtual Environment

Introduction to Kali Linux—the Hacker's Operating System: Tools in Kali Linux, Burp Suite and OWASP ZAP, How to Start OWASP ZAP.

Hack the Web Goat: Adding a Proxy to a Browser, Introducing Other Tools.

How to Inject Request Forgery: What Is Cross-Site Request Forgery? Mission Critical Injection of CSRF, Other CSRF Attacks.

How to Exploit Through Cross-Site Scripting (XSS): What Is XSS? Discovering XSS Vulnerabilities, Exploiting XSS Vulnerabilities.

Header Injection and URL Redirection: Introducing Header Injection and URL Redirection, Cross-Site Scripting Through Header Injection, Discovering Header Injection and URL Redirection Vulnerabilities.

Malicious Files: Uploading Malicious Files to Own a System, Owning a Web Site, Traditional Defacement.

Injecting Unintended XML: What Is XML External Entity Injection? Performing XML Injection in a Virtual Lab.

Experiments:

1. Implement an offensive approach to Bug Hunting
2. Create and manage Request Forgery on web pages
3. Poison Sender Policy Framework and exploit it
4. Defend against Cross Site Scripting (XSS) attacks

5. Inject Header and test URL redirection
6. Work with malicious files and Command Injection
7. Resist strongly unintended XML attacks and HTML, SQL injection
8. Earn Bounty by hunting bugs in web applications

Course Outcomes:

Upon completion of this course, the students will be able to:

CO 1. Explore web application security and common vulnerabilities. [L2]

CO 2. The basic programming constructs can be implemented using Bug Bunty Hunting. [L3]

CO 3. Apply the concepts of Cross Site Scripting and URL redirection. [L3]

CO 4. HTML and SQL concepts are used to develop applications. [L2]

CO 5. Gain practical experience through bug hunting activities. [L1]

Mapping of COs to POs:

POs/ COs	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2
CO1	3	-	-	-	-	-	-	-	-	-	-	-	-	-
CO2	-	-	3	-	-	-	-	-	-	-	-	-	2	-
CO3	-	-	3	-	2	-	-	-	-	-	-	-	1	-
CO4	-	-	-	-	3	-	-	-	-	-	-	-	2	-
CO5	-	-	-	2	2	-	-	-	-	-	-	-	-	-

TEXT BOOKS:

1. Bug Bounty Hunting for Web Security ISBN-13 (pbk): 978-1-4842-5390-8 ISBN-13 (electronic): 978-1-4842-5391-5 https://doi.org/10.1007/978-1-4842-5391-5
2. Bug Bounty Hunting Essentials: Quick-paced guide to help white-hat hackers get through bug bounty programs By Carlos A. Lozano

REFERENCE BOOKS:

1.The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws 2nd Edition by Dafydd Stuttard , Marcus Pinto.

2. The Web Application Security Guidebook" by Marco Morana.