B.Tech Computer Science and Engineering (Cyber Security)
Modified Scheme of Studies/Examination(w.e.f. Session 2023-24)
Semester VII

S. No.	Course No.	Subject	L: T:P	Hours/ Week	Credits	Examination Schedule				Duration of Exam (Hrs.)
						Major Test	Minor Test	Practical	Total	
1	PC-CS-CYS-401A	Cyber Attacks- OWASP Framework	3:0:0	3	3	75	25	0	100	3
2	HSS-403A	Universal Human Values II: Understanding Harmony	3:0:0	3	3	75	25	0	100	3
3	OEC	OEC Elective -II	3:0:0	3	3	75	25	0	100	3
4	PE-I	Elective*-I	2:0:0	2	2	75	25	0	100	3
5	PE-II	Elective* - II	2:0:0	2	2	75	25	0	100	3
6	PC-CS-CYS-405LA	Cyber Attacks- OWASP Framework Lab	0:0:2	2	1	0	40	60	100	3
7	PC-CS-CYS-407LA	Cloud Security Lab	0:0:2	2	1	0	40	60	100	3
8	PC-CS-CYS-409LA	Project-I	0:0:10	10	5	0	100	100	200	3
9	PC-CS-CYS-413LA	Industrial Training	0:0:0	0	3	0	100	0	100	
		Total		**27**	**23**	**375**	**405**	**220**	**1000**	

Code	PE-I	Code	PE-II
PE-CS-CYS- 415A	Introduction to cyber laws	PE-CS-CYS-421A	Software Testing
PE-CS-CYS-417A	Advance Computer Architecture	PE-CS-CYS-423A	Cybercrime Forensics and Digital Forensics
PE-CS-CYS-419A	Software Vulnerability Analysis	PE-CS-CYS-425A	Cloud Security

Code	OEC Elective-II
OE-CS-CYS -401	Robotics and Intelligent Systems
OE-CS-CYS-403	Ethical Hacking
OE-CS- CYS-405	Privacy and Security in IoT
OE-CS-CYS-407	Digital Electronics
OE-CS-CYS-409	Network Management and Security

Note:

***The students will choose any two departmental Electives courses and One Open Elective course out of the given elective list in VII Semester.**

****Project should be initiated in the beginning of 7th semester, and should be completed by the end of 7th semester with good Report and power-point Presentation etc.**

*****4-6 weeks hand on training completed after 6th Semester Exams.**

PC-CS-CYS-401A	Cyber Attacks- OWASP Framework						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
3	**0**	**0**	**3**	**75**	**25**	**100**	**3 Hours**
Purpose	To understand web application security course based on OWASP Top 10 web application security risks.						
Course Outcomes (CO)							
CO1	Awareness about OWASP Top 10 web application security risks.						
CO2	Understanding of the most critical security risks to web applications.						
CO3	Identify and mitigate the ten most critical security risks by reviewing vulnerable source code.						
CO4	Understand the need of writing the secure code.						

Unit- I

Getting Started with OWASP, Application Security Risks, OWASP Top 10 Application Security Risks, Introduction to Web Application Security (OWASP A02:2021 Cryptographic Failures, OWASP A04:2021—Insecure Design).

Unit-II

User Authentication (OWASP A07:2021—Identification and Authentication Failures, OWASP A03:2021—Injection, OWASP A02:2021—Cryptographic Failures), Function and Data Access Control (OWASP A01:2021—Broken Access Control).

Unit-III

SQL Injection (OWASP A03:2021—Injection), Cross-Site Scripting (XSS) (OWASP A08:2021—Software and Data Integrity Failures), Handling Data from an Untrusted Source (OWASP A09:2021—Security Logging and Monitoring Failures, A10:2021—Server-Side Request Forgery).

Unit-IV

Processing of Composite Data (OWASP A08:2021—Software and Data Integrity Failures), Configuration Errors (OWASP A05:2021—Security Misconfiguration, A06:2021— Vulnerable and Outdated Components).

Miscellaneous topics: Cross Site Request Forgery (CSRF), JWT security, session hijacking, Local File Inclusion (LFI), Remote File Inclusion (RFI).

Suggested Books:

- OWASP. Top 10 the Most Critical Web Application Security Risks. 2021. Available online: https://owasp.org/Top10/ (accessed on 15 January 2023).
- Troiano, Ernesto, Maurizio Ferraris, and John Soldatos. "Security challenges for the critical infrastructures of the financial sector." Cyber-physical threat intelligence for critical infrastructures security (2020).

HSS-403A	Universal Human Values II: Understanding Harmony						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**MinorTest**	**Total**	**Time**
3	**0**	**0**	**3.0**	**75**	**25**	**100**	**3 Hours**
Purpose	Purposeandmotivationforthecourse,recapitulationfromUniversalHumanValues-I						
CourseOutcomes(CO)							
CO1	Developmentofaholisticperspectivebasedonself-explorationabout						
CO2							
CO3	Strengtheningofself-reflection.						
CO4	Developmentofcommitmentandcouragetoact.						

Module1:CourseIntroduction-Need,BasicGuidelines, ContentandProcessforValueEducation

1. Purposeandmotivationforthecourse,recapitulationfromUniversalHumanValues-I
2. Self-Exploration–what isit? - Its content and process;'Natural Acceptance' andExperiential Validation-as the process forself-exploration
3. ContinuousHappinessandProsperity- AlookatbasicHumanAspirations
4. Rightunderstanding,RelationshipandPhysicalFacility- thebasicrequirementsforfulfilmentofaspirationsofeveryhumanbeingwiththeircorrectpriority
5. UnderstandingHappinessandProsperitycorrectly-Acriticalappraisalofthecurrentscenario
6. MethodtofulfiltheabovehumanaspirationsunderstandingandlivinginharmonyatvariouslevelsIncludepracticesessionstodiscussnaturalacceptanceinhumanbeingastheinnateacceptanceforlivingwithresponsibility(livinginrelationship,harmonyandco-existence)ratherthanasarbitrarinessinchoicebasedonliking-disliking

Module2:UnderstandingHarmonyintheHumanBeing-HarmonyinMyself!

1. Understandinghumanbeingasaco-existenceofthesentient'I'andthematerial'Body'
2. UnderstandingtheneedsofSelf('I') and 'Body'-happinessandphysicalfacility
3. UnderstandingtheBodyasaninstrumentof'I'(Ibeingthedoer,seer andenjoyer)
4. Understandingthecharacteristicsandactivitiesof'I'andharmonyin'I'
5. Understanding the harmony of I with the Body: Sanyam and Health; correct appraisal of Physical needs,meaningofProsperityindetail
6. Programstoensure SanyamandHealth.

Include practice sessions to discuss the role others have played in making material goods available tome. Identifying from one's own life. Differentiate between prosperity and accumulation. Discussprogramforensuringhealthvs dealingwithdisease

Module 3: Understanding Harmony in the Family and Society- Harmony in Human-HumanRelationship

1. Understanding values in human-human relationship; meaning of Justice (nine universal values inrelationships)andprogramforitsfulfilmenttoensuremutualhappiness;TrustandRespectasthefoundationalvaluesofrelationship
2. UnderstandingthemeaningofTrust;Differencebetweenintentionandcompetence

3. Understanding the meaning of Respect, Difference between respect and differentiation; the othersalientvaluesinrelationship
4. Understanding theharmony inthesociety(societybeinganextensionoffamily): Resolution,Prosperity,fearlessness(trust)and co-existence ascomprehensive Human Goals
5. Visualizing a universal harmonious order in society- Undivided Society, Universal Order- fromfamilytoworldfamily.

Include practice sessions to reflect on relationships in family, hostel and institute as extended family,reallifeexamples,teacher-studentrelationship,goalofeducationetc.Gratitudeasauniversalvalueinrelationships.Discusswithscenarios.Elicitexamplesfromstudents'lives

Module4:UnderstandingHarmonyintheNatureandExistence-WholeexistenceasCoexistence

1. Understandingtheharmony intheNature
2. Interconnectednessandmutualfulfilmentamongthefourordersofnature- recyclabilityandself-regulationinnature
3. UnderstandingExistenceasCo-existenceof mutuallyinteractingunitsinall-pervasivespace
4. Holisticperceptionofharmonyatalllevels ofexistence.

Include practice sessions to discuss human being as cause of imbalance in nature (film "Home" canbeused),pollution,depletionofresources androle oftechnologyetc.

Module5: ImplicationsoftheaboveHolisticUnderstandingofHarmonyonProfessionalEthics

1. Naturalacceptance ofhumanvalues
2. Definitiveness ofEthicalHumanConduct
3. BasisforHumanisticEducation,HumanisticConstitutionandHumanisticUniversalOrder
4. Competenceinprofessionalethics:a.Abilitytoutilizetheprofessionalcompetenceforaugmenting universal human order b. Ability to identify the scope and characteristics of people-friendly and eco-friendly production systems, c. Ability toidentify and develop appropriatetechnologiesandmanagementpatternsforabove productionsystems.
5. Casestudiesoftypicalholistictechnologies,managementmodelsandproductionsystems
6. Strategy for transition from the presentstate to Universal Human Order: a.At the level ofindividual: as socially and ecologically responsible engineers, technologists and managers b. Atthe levelofsociety:asmutuallyenrichinginstitutionsandorganizations
7. Sumup.

IncludepracticeExercisesandCaseStudieswillbetakenupinPractice(tutorial)Sessionseg.todiscusstheconductas anengineerorscientistetc.

READINGS:

TextBook

1. HumanValuesand ProfessionalEthicsbyRRGaur,RSangal,GP Bagaria,ExcelBooks,New Delhi,2010

ReferenceBooks

1. JeevanVidya:EkParichaya, ANagaraj, JeevanVidyaPrakashan, Amarkantak,1999.
2. HumanValues,A.N.Tripathi,NewAgeIntl.Publishers,NewDelhi,2004.

3. TheStoryofStuff(Book).
4. TheStoryofMyExperimentswithTruth-byMohandas KaramchandGandhi
5. SmallisBeautiful-E.FSchumacher.
6. SlowisBeautiful-CecileAndrews
7. EconomyofPermanence-JCKumarappa
8. BharatMeinAngrejiRaj-PanditSunderlal
9. RediscoveringIndia -byDharampal
10. HindSwarajor IndianHomeRule-byMohandas K.Gandhi
11. IndiaWinsFreedom-MaulanaAbdulKalamAzad
12. Vivekananda-RomainRolland(English)
13. Gandhi-RomainRolland(English)

MODEOFCONDUCT

Lecture hours are to be used for lecture/practice sessions.

Lectureshoursaretobeusedforinteractivediscussion, placingtheproposalsaboutthetopicsathandandmotivatingstudents toreflect,explore andverifythem.

Practicehoursaretobeusedforpracticesessions.

Whileanalysinganddiscussingthetopic,thefacultymentor'sroleisinpointingtoessentialelementsto help in sorting them out from the surface elements. In other words, help the students explore theimportantorcriticalelements.

In the discussions, particularly during practice sessions, the mentor encourages the studentto connect with one's own self and do self-observation, self-reflection and self-exploration. Scenariosmay be used to initiate discussion. The student is encouraged to take up" ordinary" situations ratherthan" extra-ordinary" situations. Such observations and their analyses are shared and discussed withotherstudents andfacultymentor,inagroupsitting.

Practice experiments are important for the course. The difference is that the laboratoryis everyday life, and practical are how you behave and work in real life. Depending on the nature oftopics, worksheets, home assignment and/or activity are included. The practice sessionswould also provide support to a student in performing actions commensurate to his/her beliefs. It isintendedthatthiswouldleadtodevelopmentofcommitment,namelybehavingandworkingbasedonb asichuman values.

It is recommended that this content be placed before the student as it is, in the form of a basicfoundation course, without including anything else or excluding any part of this content. Additionalcontentmaybe offeredinseparate,highercourses.

Thiscourseistobetaughtbyfacultyfromeveryteachingdepartment,includingHSSfaculty.Teacherprepar ationwithaminimumexposuretoatleastone8-dayFDPonUniversalHumanValuesisdeemedessential.

ASSESSMENT:

This is a compulsory credit course. The assessment is to provide a fair state of development of thestudent, so participation in classroom discussions, self-assessment, peer assessment etc. will be usedinevaluation.

Example:

Assessmentby
facultymentor:5 marks
Self-assessment:5 marks
Assessmentbypeers:5 marks
Sociallyrelevantproject/GroupActivities/Assignments:10 marks
SemesterEndExamination: 75marks
Theoverallpasspercentageis40%. Incasethestudentfails,he/shemustrepeatthecourse.

OE-CS-CYS-401	Robotics and Intelligent Systems						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
3	**0**	**0**	**3**	**75**	**25**	**100**	**3**
Purpose	To impart understanding of the main abstractions and reasoning for Robotics and Intelligent Systems						
Course Outcomes (COs)							
CO1	Understand the basic terminologies in Robotics to develop intelligent systems						
CO2	Apply the random search and heuristic search for intelligent systems.						
CO3	Understand the abstractions and reasoning for intelligent systems						
CO4	Apply the rule-based methods in intelligent systems						
CO5	Identify the characteristics and architectures of algorithms of multi agent systems						
CO6	Identify different application areas of Intelligent Systems						

UNIT-I

Introduction to robotics- History, growth; Robot applications- Manufacturing industry, defense, rehabilitation, medical, Robot mechanisms, type of robots and use of robots in different area.

UNIT-II

Degree of freedom, classification and specifications of Robots, controller, actuator and drives. Sensors in robot – Touch Sensors-Tactile sensor – Proximity and range sensors. Force sensor-Light sensors, Pressure sensors, Introduction to Machine Vision and Artificial Intelligence.

U**NIT-III**

Intelligent Systems: Knowledge acquisition, Computational intelligence, Rule-based systems, Forward-chaining (a data-driven strategy), Conflict resolution, Backward chaining (a goal-driven strategy), Sources of uncertainty, Bayesian updating, Certainty theory.

UNIT-IV

Possibility theory: fuzzy sets and fuzzy logic, Object-oriented systems, Data abstraction, Inheritance, Encapsulation, Unified Modeling Language (UML), Dynamic (or late) binding. **Key Application Areas:** Expert System, Decision Support Systems, **Deep Learning:** Speech and vision, natural Language processing, Information Retrieval, Semantic Web.

SUGGESTED BOOKS:

1. Artificial Intelligence RB Mishra, PHI
2. Introduction to Artificial Intelligence, Charnaik, Pearson.
3. Artificial Intelligence by Elaine Rich, Kevin Knight and Shivashankar B Nair, Tata McGraw Hill.
4. Introduction to Artificial Intelligence and Expert Systems by Dan W Patterson, Pearson Education.

5. Artificial Intelligence : Building Intelligent Systems, KULKARNI, Parag , REPRINT, PHI.
6. CrinaGrosan, Ajith Abraham, “Intelligent Systems: A Modern Approach “,Springer-Verlag, 2011
7. Bogdan M. Wilamowski, J. David Irwin, “The Industrial Electronics Handbook. Second Edition: Intelligent Systems”, CRC Press, 2011
8. Abraham-Kandel, Gideon-Langholz, “Hybrid-Architectures for Intelligent Systems”, CRC-Press, 1992
9. Augmented Human, PAPAGIANNIS, Helen ,ist print, SPD.

10. Ian Goodfellow, YoshuaBengio and Aaron Courville, "Deep Learning", MIT Press, http://www.deeplearningbook.org

OE-CS-CYS-403	Ethical Hacking						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
3	**0**	**0**	**3**	**75**	**25**	**100**	**3 Hrs.**
Purpose	The course teaches beginners about computer systems with the permission of the organization. People who have a keen interest in the field of technology can opt for this course. Ethical hacking is a process wherein professionals use the vulnerabilities of a network/ system to detect intrusions from malicious hackers.						
	Course Outcomes						
CO 1	To gain knowledge about Ethical hacking and penetration testing.						
CO 2	To learn about various types of attacks, attackers and security threats and vulnerabilities present in the computer system.						
CO 3	To examine how social engineering can be done by attacker to gain access of useful & sensitive information about the confidential data.						
CO 4	To learn about cryptography, and basics of web application attacks.						

Unit-I Ethical Hacking: Introduction, Networking & Basics, Foot Printing, Google Hacking, Scanning, Windows Hacking, Linux Hacking, Trojans & Backdoors, Virus & Worms.

Unit-II Security operations center(SOC), SOC framework, SOC tools, what is QRadar, Incident Detection and Investigation with QRadar, Incident Responder process.

Unit-III Wifi hacking, firewall and honeypots, Snort introduction, Snort implementation, pentration testing, hacking web server, SQL injection, exploit writing in python, Format string

Unit-IV Reverse Engineering, Email Hacking, Incident Handling & Response, Bluetooth Hacking, Mobile Phone Hacking Basic ethical hacking tools and usage of these tools in a professional environment. Legal, professional and ethical issues likely to face the domain of ethical hacking. Ethical responsibilities, professional integrity and making appropriate use of the tools and techniques associated with ethical hacking.

Suggested Books:

Hacking: The Art of Exploitation, Jon Erickson, 2nd edition, No Starch Press
The Basics of Hacking and Penetration Testing, Patrick Engebretson, 2nd edition, Syngress
The Web Application Hacker's Handbook, DafyddStuttard, 2nd edition, Wiley

OE-CS-CYS-405	Privacy and Security in IoT						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
3	**0**	**0**	**3**	**75**	**25**	**100**	**3 Hrs.**
Purpose	ToexplorethePrivacyPreservationandTrustModelsinInternetofThings(IoT)						
Course Outcomes (CO)							
CO1	Identifytheareasof cybersecurityforthe InternetofThings.						
CO2	Assessdifferent InternetofThingstechnologiesandtheirapplications.						
CO3	Customizerealtimedata forIoTapplications.						
CO4	Solve IoTsecurityproblems usinglightweightcryptography.						

UNITI

IntroductiontoIoT –CyberPhysicalSystems: IoTand cyber-physicalsystems,IoT security(vulnerabilities, attacks, andcountermeasures), security engineeringfor IoTdevelopment, IoTsecuritylifecycle. **IoTasInterconnectionof Threats:** NetworkRobustnessofInternetofThings-SybilAttackDetectioninVehicularNetworks-Malware PropagationandControlinInternetofThings-Solution-BasedAnalysisofAttackVectorsonSmartHomeSystems

UNITII

CryptoFoundations: Blockciphers,messageintegrity,authenticatedencryption, hashfunctions,Merkletrees,ellipticcurves, public-keycrypto (PKI), signaturealgorithms

Privacy PreservationforIoT: Privacy Preservation Data Dissemination- Privacy Preservation Data Dissemination- Social Features forLocationPrivacyEnhancementinInternetof Vehicles-LightweightandRobustSchemes forPrivacy ProtectioninKeyPersonalIoTApplications:MobileWBSNandParticipatorySensing

UNITIII

TrustModelsforIoT: Authentication in IoT- Computational Security for the IoT- Privacy-Preserving Time Series DataAggregation-SecurePathGenerationSchemefor Real-TimeGreenInternetofThings-SecurityProtocols for IoT Access Networks- Framework for Privacy and Trust in IoT- Policy-Based Approach for InformedConsentinInternet of Things.

UNITIV

InternetofThingsSecurity: Securityand Impactofthe InternetofThings(IoT)onMobileNetworks-NetworkingFunctionSecurity-IoT NetworkingProtocols,SecureIoTLowerLayers,SecureIoTHigherLayers,SecureCommunicationLinksinIoTs, Back-endSecurity-SecureResourceManagement,SecureIoT Databases,SecurityProducts-Existing TestbedonSecurityandPrivacyofIoTs,CommercializedProducts.

Text Books:

1. Hu, Fei. Security and privacy in Internet of things (IoTs): Models, Algorithms, and

Implementations, 1st edition, CRC Press, 2016.
2. Russell, Brian, and Drew Van Duren. Practical Internet of Things Security, 1st edition, Packt Publishing Ltd, 2016.

REFERENCES:

1. White House O. Security of things: An implementers' guide to cyber-security for internet of things devices and beyond, 1st edition, NCC Group, 2014
2. Da Costa, Francis, and Byron Henderson. Rethinking the Internet of Things: a scalable approach to connecting everything, 1st edition, Springer Nature, 2013.

Code: OE-CS-CYS-407	**Digital Electronics**						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
3	**0**	**0**	**3**	**75**	**25**	**100**	**3 Hour**
Purpose	Understanding the different number systems used in computerized system and codes used to represent the digits and fundamental of arithmetic operation using each number system and codes.						
Course Outcomes (CO)							
CO1	Verify and analyze the input/output data of each logic gate and circuits such as adders, counters, coders, etc.						
CO2	Analyse the basic operation of memory cell and its limitations in circuit designing.						
CO3	Apply the digital circuit design concept in developing basic component of computer organization, projects or experiments.						
CO4	Learn synchronous and asynchronous modes of machines						

Unit-I

Number System and Boolean Algebra

Review of number system; types and conversion, codes. Boolean algebra: De-Morgan's theorem, switching functions, Prime Implicants and Essential Prime Implicants definition and simplification using K-maps up to 5 variables & Quine McCluskey method.

Unit-II

Combinational Circuits

Introduction to Logic Gates: AND, OR, NOT, NAND, NOR, EX-OR, EX-NOR and their combinations. Design of adder, subtractors, comparators, code converters, encoders, decoders, multiplexers and de-multiplexers, Function realization using gates & multiplexers.

Unit-III

Synchronous Sequential Circuits

Introduction to Latches and Flip flops – SR, D, JK and T. Design of synchronous sequential circuits – Counters, shift registers. Finite State Machine Design, Mealy, Moore Machines, Analysis of synchronous sequential circuits; state diagram; state reduction; state assignment with examples

UNIT – IV

Asynchronous Sequential Circuits

Analysis of asynchronous sequential machines, state assignment, asynchronous design problem**, Memories and Logic Families:**

Memories: ROM, RAM, PROM, EPROM, Cache Memories, PLA, PLD, FPGA, digital logic families: TTL, ECL, CMOS.

Reference Books:

Mano, Morris. "Digital logic." *Computer Design. Englewood Cliffs Prentice-Hall* (1979).

Kumar, A. Anand. *Fundamentals Of Digital Circuits 2Nd Ed.* PHI Learning Pvt. Ltd., 2009.

Taub, Herbert, and Donald L. Schilling. *Digital integrated electronics*. New York: McGraw-Hill, 1977.

OE-CS-CYS-409	Network Management and Security						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
3	**0**	**0**	**3**	**75**	**25**	**100**	**3 Hrs.**
Purpose	To enable students to learn the various security standards set by the global industry. The various security applications that are used by industry.						
	Course Outcomes						
CO 1	Discuss the basic concepts of network security and various cryptographic algorithms.						
CO 2	Describe how wireless security provided to information						
CO 3	Discuss the Network Management Policy						
CO 4	Discuss security and law along with Internet Governance and Email policy.						

Unit-I. Analysis of Goals: Analyzing business & technical goals Characterizing a Network, Network Topology & Addressing, Hierarchical Networks, Redundant Topologies, Designing Campus and Enterprise Topologies, Network layer addressing, Protocols & Physical Design, Switching Protocols, Routing Protocols , Cable Technologies , Device Selection

Unit-II: Remote Access & WAN topologies, LAN technologies, LAN design Principles, PPP, Modem, DSL access, SONET, Frame Relay. ATM, WAN design Principles, Network Management I SNMP MIB

Unit-III

Email privacy: Pretty Good Privacy (PGP) and S/MIME.IP Security Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management.

Unit-IV

Basic concepts of SNMP, SNMPv1 Community facility and SNMPv3. Intruders, Viruses and related threats. Firewall Design principles, Trusted Systems. Intrusion Detection Systems.

Suggested Books:

Jianguo Ding, Advances in Network Management, Auerbach Publication, 2009, ISBN-10: 1420064525, ISBN-13: 978-1420064520 (available on-line)

Alexander Clemm, Network Management Fundamentals, Cisco Press (2007), ISBN 1-58720-137-2

P. Oppenheimer: Top Down Network Design 3rd edition and J Richard Burke

Network Management: Concepts and Practice, A Hands on Approach.

PE-CS-CYS-415A	Introduction to cyber laws						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
2	**0**	**0**	**2**	**75**	**25**	**100**	**3 Hours**
Purpose	The course deals with all the aspects of Cyber law as per Indian/IT act. It also covers overview of Cyber Ethics, Intellectual Property Right and Trademark Related laws with respect to Cyber Space.						
Course Outcomes (CO)							
CO 1	To give overview of Cyber Ethics, Intellectual Property Right and Trademark Related laws with respect to Cyber Space.						
CO 2	To analyze and evaluate existing legal framework and laws on cyber security.						
CO 3	To analyze and evaluate the Intellectual rights and copyrights.						
CO 4	To understand cyber ethics.						

Unit-1

Introduction to Cybercrime and cyber law: Cyber Crimes Categories and kinds, Evolution of the IT Act, IT Act, 2000, various authorities under IT Act and their powers. Penalties & Offences, amendments

Unit-2

Jurisdiction and Ecommerce: Case Laws on Cyber Space Jurisdiction and Jurisdiction issues under IT Act, E – commerce and Laws in India, Digital / Electronic Signature in Indian Laws.

Unit-3

Intellectual rights and copyrights: Intellectual Property Rights, Domain Names and Trademark Disputes, Copyright in Computer Programmes, Concept of Patent Right, Sensitive Personal Data or Information in Cyber Law, Cyber Law an International Perspective.

Unit-4

Cyber Ethics: Cyber Ethics and Code, Net Neutrality, Free speech and Censorship in Cyberspace, Intellectual Property in Cyberspace, Privacy Rights and Surveillance.

Suggested Books:

1. Sushma Arora, Raman Arora, Cyber Crimes & Laws, 4th Edition 2021, Publisher: Taxmann, ISBN-10: 9390712491
2. N S Nappinai, Technology Laws Decoded, 1st Edition, Publisher: Lexis Nexis, ISBN: 9789350359723
3. Suresh T. Vishwanathan, The Indian Cyber Law, Bharat Law House New Delhi
4. P.M. Bukshi and R.K. Suri, Guide to Cyber and E –Commerce Laws, Bharat Law House, New Delhi
5. Rodney D. Ryder, Guide to Cyber Laws; Wadhwa and Company, Nagpur

Note: The Examiner will be given the question paper template and will have to set the question paper according to the template provided along with the syllabus.

PE-CS-CYS-417A	Advance Computer Architecture						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
2	**0**	**0**	**2**	**75**	**25**	**100**	**3 Hour**
Purpose	To enable students to learn various computational models, design paradigms of advanced computer architecture, parallelism approaches and techniques for static and dynamic interconnections.						
Course Outcomes (CO)							
CO1	Classify and interpret various paradigms, models and micro-architectural design of advanced computer architecture as well as identify the parallel processing types and levels for achieving optimum scheduling						
CO2	Identify the roles of VLIW & superscalar processors and branch handling techniques for performance improvement						
CO3	Analyze and interpret the basic usage of various MIMD architectures and relative importance of various types of static and dynamic connection networks for realizing efficient networks.						
CO4	Examine the various types of processors and memory hierarchy levels and cache coherence problem including software and hardware-based protocols to achieve better speed and uniformity.						

Unit-I

Computational Model: Basic computational models, evolution and interpretation of computer architecture, concept of computer architecture as a multilevel hierarchical framework, classification of parallel architectures, Relationships between programming languages and parallel architectures. Parallel Processing: Types and levels of parallelism, Instruction Level Parallel (ILP) processors, dependencies between instructions, principle and general structure of pipelines, performance measures of pipeline, pipelined processing of integer, Boolean, load and store instructions, VLIW architecture, Code Scheduling for ILP Processors - Basic block scheduling, loop scheduling, global scheduling.

Unit-II

Superscalar Processors: Emergence of superscalar processors, Tasks of superscalar processing – parallel decoding, superscalar instruction issue, shelving, register renaming, parallel execution, preserving sequential consistency of instruction execution and exception processing, comparison of VLIW & superscalar processors. Branch Handling: Branch problem, Approaches to branch handling – delayed branching, branch detection and prediction schemes, branch penalties, multiway branches, guarded execution.

Unit-III

MIMD Architectures: Concepts of distributed and shared memory MIMD architectures, UMA, NUMA, CCNUMA & COMA models, problems of scalable computers. Static connection networks: Linear array, ring, chordal ring, barrel shifter, star, tree, mesh and torus, fat Tree, systolic array, barrel shifter, hypercubes and Cube connected cycles. Dynamic interconnection networks: single shared buses, comparison of bandwidths of locked, pended & split transaction buses, arbiter logics, crossbar networks, multistage networks, omega networks, butterfly.

UNIT – IV

Processors and Memory Hierarchy: Advanced processor technology, memory hierarchy technology and virtual memory technology. Cache Coherence and Synchronization Mechanisms: Cache coherence problems, hardware based protocols – snoopy cache protocols, directory schemes, hierarchical cache coherence protocols, software based protocols.

Reference Books:

1. D.Sima, T.Fountain, P.Kasuk, Advanced Computer Architecture-A Design Space Approach, Pearson Education.
2. Kai Hwang and NareshJotwani, Advanced Computer Architecture-Parallelism, Scalability, Programmability, McGraw Hill.
3. M.J. Quinn, Parallel Computing: Theory and Practice, Second Edition, McGraw Hill.
4. J. L. Hennessy and D. A. Patterson, Computer Architecture: A Quantitative approach, Morgan Kaufmann/Elsevier.
5. T.G. Lewis and H. EI- Rewini, Introduction to parallel computing, Prentice Hall.
6. Nicolas Carter, Computer Architecture, McGraw Hill.

PE-CS-CYS-419A	Software Vulnerability Analysis						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
2	**0**	**0**	**2**	**75**	**25**	**100**	**3 Hours**
Purpose	Identification and quantification of security weaknesses, primarily in source code and executables.						
Course Outcomes (CO)							
CO1	Explain computer security problem and identify why broken software lies at its heart.						
CO2	Develop and apply software validation and verification techniques to test security vulnerabilities.						
CO3	Develop case studies to think like an attacker to expose security vulnerabilities in software systems.						
CO4	Relate security testing and verification to risk analysis to address continued resilience when a cyber-attack takes place.						

Unit- I

Classic security goals (confidentiality, integrity, etc.), Threats and threat exposure, Vulnerability categories, Audit overview, Design reviews, Fundamental design flaws, Threat modeling.

Unit-II

Review/Audit process, Audit strategies, Memory corruption: buffer overflows, heap overflows, global and static data, shellcode, protection mechanisms.

Unit-III

C/C++ language issues, Expression evaluation, Type conversions, Common mistakes, String handling issues, String encodings, Metacharacter handling and injection issues, String functions, Hex encoding.

Unit-IV

Auditing techniques for source code and binary analysis, Hardware vulnerabilities (Specter, Meltdown, etc.)

Suggested Books:

- Computer Security: Art and Science, 2nd edition. Matt Bishop. Addison-Wesley, 2019, ISBN-13: 978-0-321-71233-2.

PE-CS-CYS-421A	Software Testing						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
2	**0**	**0**	**2**	**75**	**25**	**100**	**3 Hrs.**
Purpose	**To provide an understanding of concepts and techniques for testing software and assuring its quality.**						
	Course Outcomes						
CO 1	Expose the criteria and parameters for the generation of test cases.						
CO 2	Learn the design of test cases and generating test cases.						
CO 3	Be familiar with test management and software testing activities and V&V activities.						
CO 4	Be exposed to the significance of software testing in web and Object orient techniques.						

Unit-I

Introduction: Overview of software evolution, SDLC, Testing Process, Terminologies in Testing: Error, Fault, Failure, Verification, Validation, Difference between Verification and Validation, Definition of software testing, test cases, test oracles, testing process, limitations of testing.

Unit-II

Functional Testing: Boundary Value Analysis, Equivalence Class Testing, Decision Table Based Testing, Cause Effect Graphing Technique.

Structural Testing: Path testing, DD-Paths, Cyclomatic Complexity, Graph Metrics, Data Flow Testing, Mutation testing.

Unit-III

Reducing the number of test cases: Prioritization guidelines, Priority category, Scheme, Risk Analysis, Regression Testing and Slice based testing.

Testing Activities: Unit Testing, Levels of Testing, Integration Testing, System Testing, Debugging, Domain Testing.

Unit-IV

Overview of SQM: Concepts of Software Quality, quality attributes, software quality models: McCall, Boehm, ISO-9000, CMM.

Misellaneous Topics: Stress testing, Adhoc testing, Buddy testing, Exploratory testing, Agile and extreme testing.

Suggested Books:

- Naresh Chauhan, "Softearw Testing Principles and Practices" Oxford publications, 2012.
- William Perry, "Effective Methods for Software Testing", John Wiley & Sons, New York, 1995.
- CemKaner, Jack Falk, Nguyen Quoc, "Testing Computer Software", Second Edition, Van Nostrand Reinhold, New York, 1993.
- Boris Beizer, "Software Testing Techniques", Second Volume, Second Edition, Van Nostrand Reinhold, New York, 1990.
- Louise Tamres, "Software Testing", Pearson Education Asia, 2002
- Roger S. Pressman, "Software Engineering – A Practitioner's Approach", Fifth Edition, McGraw-Hill International Edition, New Delhi, 2001.
- Boris Beizer, "Black-Box Testing – Techniques for Functional Testing of Software and Systems", John Wiley & Sons Inc., New York, 1995.
- K.K. Aggarwal & Yogesh Singh, "Software Engineering", New Age International Publishers, New Delhi, 2003.
- Marc Roper, "Software Testing", McGraw-Hill Book Co., London, 1994.

PE-CS-CYS-423A	Cybercrime Forensics and Digital Forensics						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
2	**0**	**0**	**2**	**75**	**25**	**100**	**3 Hours**
Purpose	Understanding of digital logic, operating system concepts, Computer hardware knowledge.						
Course Outcomes (CO)							
CO 1	Describe Forensic science and Digital Forensic concepts						
CO 2	Understand of preliminaries operating systems and their artefacts.						
CO 3	Interpret the cyber pieces of evidence, Digital forensic process model and their legal perspective.						
CO 4	Demonstrate various forensic tools to investigate the cybercrime and to identify the digital pieces of evidence						

Unit-1

Introduction: Introduction to Digital Forensics, Definition and types of cybercrimes, Computer virus, and computer worm, Trojan horse, trap door, super zapping, logic, social media crimes, intellectual property crimes, cyber pornography& child pornography, cyber terrorism, hate speech and cyber security, hacking and cracking, credit card and ATM frauds, web technology, cryptography, emerging digital crimes and modules.

OS System and Artifacts: Definition and Cardinal Rules, Windows Systems and Artifacts: Introduction, Windows File Systems, New Technology File System, File System Summary, Registry, Event Logs, Prefetch Files, Shortcut Files, Windows Executables.

Unit-II

Linux Systems and Artifacts: Introduction, Linux File Systems, File System Layer, File Name Layer , Metadata Layer, Data Unit Layer, Journal Tools, Deleted Data, Linux Logical Volume Manager, Linux Boot Process and Services, Linux System Organization and Artifacts, Partitioning, File system Hierarchy, Ownership and Permissions, File Attributes, Hidden Files, User Accounts , Home Directories, Shell History, Logs, User Activity Logs, Syslog, Command Line Log Processing, Scheduling Tasks.

Unit-III

Digital Forensics Process Model: The digital forensic process, Locard's exchange principle, Scientific models, Introduction to cybercrime scene, Documenting the scene and evidence, maintaining the chain of custody, forensic cloning of evidence, Live and dead system forensic, hashing concepts to maintain the integrity of evidence, legal issues.

Unit-IV

Forensic Tools and Processing of Electronic Evidence: Evaluating Computer Forensics Tool Needs, Types of Computer Forensics Tools, Tasks Performed by Computer Forensics Tools, Computer Forensics Software Tools, Command-Line Forensics Tools, UNIX/Linux Forensics Tools, finding deleted data, hibernating files, examining window registry, recycle bin operation, understanding of metadata, Restore points and shadow copies. Case Studies: Understanding of Internet resources, Web browser, Email header forensic, social networking sites

Text and Reference Books:

1. C. Altheide& H. Carvey Digital Forensics with Open-Source Tools, Syngress

2. Bill Nelson, Amelia Phillips, Christopher Steuart, “Guide to Computer Forensics and Investigations”, Fourth Edition

3. www.nptel.com

PE-CS-CYS-425A	**Cloud Security**						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
2	**0**	**0**	**2**	**75**	**25**	**100**	**3 Hour**
Purpose	To enable students to learn various computational models, design paradigms of advanced computer architecture, parallelism approaches and techniques for static and dynamic interconnections.						
Course Outcomes (CO)							
CO1	Classify and interpret various paradigms, models and micro-architectural design of advanced computer architecture as well as identify the parallel processing types and levels for achieving optimum scheduling						
CO2	Identify the roles of VLIW & superscalar processors and branch handling techniques for performance improvement						
CO3	Analyze and interpret the basic usage of various MIMD architectures and relative importance of various types of static and dynamic connection networks for realizing efficient networks.						
CO4	Examine the various types of processors and memory hierarchy levels and cache coherence problem including software and hardware-based protocols to achieve better speed and uniformity.						

Unit - 1

Introduction to AWS Security by Design, AWS Key Management Best Practices, A Deep Dive into AWS Encryption Services, Security at Scale: Logging in AWS, AWS WAF, AWS Security Incident Response.

Unit - 2

Common attacks on cloud infrastructure: Unauthorized Access, SQL injection, XSS, Misconfiguration, DOS - DDOS, Data Loss/Leakage, Data Privacy/Confidentiality, Incident Response, counter measure to protect cloud infrastructure.

Unit - 3

Data Protection for Cloud Infrastructure and Services: Understand the Cloud based Information Life Cycle, Data protection for Confidentiality and Integrity, Data protection laws of India, Common attack vectors and threats, Data Protection Strategies.

Unit - 4

Monitoring, Auditing and Management: Proactive activity monitoring, Incident Response, Monitoring for unauthorized access, malicious traffic, abuse of system privileges, intrusion detection, events and alerts.

Reference books

Securing The Cloud: Cloud Computing Security Techniques and Tactics by Vic (J.R.) Winkler (Syngress/Elsevier) - 978-1-59749-592-9 o

Cloud Computing Design Patterns by Thomas Erl (Prentice Hall) - 978-0133858563

PC-CS-CYS-405LA	Cyber Attacks- OWASP Framework Lab						
Lecture	**Tutorial**	**Practical**	**Credit**	**Minor Test**	**Practical**	**Total**	**Time**
0	**0**	**2**	**1**	**40**	**60**	**100**	**3 Hours**
Purpose	Understand the OWASP Top 10 and how to use them to minimize risk.						
Course Outcomes (CO)							
CO1	Apply the OWASP Top 10 to ensure your applications minimize the security risks in the list.						
CO2	Explore how Web Applications are built and delivered on top of the HTTP protocol.						
CO3	Explore threat agents, attack vectors, and impact of the ten most critical web application security risks.						
CO4	Explore common exploitation techniques used to test software security.						

LIST OF PRACTICALS*:*

1. **Lab1: Introduction to Web Application Security-** In this lab, there is creation of an environment for testing the security of WWW applications and for performing basic tasks such as data preview and modification of the transmitted HTTP requests. Virtual laboratories in this topic are based on OWASP A02:2021—Cryptographic Failures and OWASP A04:2021—Insecure Design. The exercises involved in this lab are-- Response Headers Preview (*), Manipulating HTTP Parameters (*), Launch and Configuration of Proxy in a browser (**), Automatic Application Scan (*), Modification of HTTP Requests (*), Repeating HTTP Request (*), Finding the Right Parameter Value by Brute Force Method (**).

2. **Lab2: User Authentication-** This topic concerns authentication-related attacks. Authentication describes the procedure to verify one's identity. On most websites, it is encountered in the form of a username and password combination that is needed to log in. Session management, on the other hand, comes into play when we are successfully authenticated. Upon login, a unique session key is generated. This unique key ensures that our logged-in session is held upright as we browse the application, so we do not have to re-authenticate each time we switch the endpoint. Broken authentication denotes that there is an issue with the authentication or the way that the session is handled. In this module, students can detect broken authentication using manual methods and can exploit them using automated tools with password lists and dictionary attacks. They can examine and compromise session tokens. Virtual laboratories in this topic are based on OWASP A07:2021—Identification and Authentication Failures, OWASP A03:2021—Injection, and OWASP A02:2021—Cryptographic Failure and consist of five exercises, which are described as: Low-Complexity User Password (**), Weak Randomness Session Identifier (**), Client-Side Authentication (*), Incorrect password reset implementation (**), User Enumeration Based on Response Time (**).

3. **Lab3: Function and Data Access Control-** In this module, students are introduced to the weaknesses and vulnerabilities available in broken access control. Access control, also known as authorization (not to be confused with authentication), is a process that determines whether users can gain access to a resource. Authorization is a basic security service that appears in most applications. Decisions regarding access control are generally enforced on the basis of rules (called policies) set down by the user. Virtual laboratories in this topic are based on OWASP A01:2021—Broken Access Control and consist of the five exercises described in detail below as: Access to Hidden Pages (**), Security Flaw in Access to API (**), HTTP Parameter Manipulation (**), Path Traversal Vulnerability (**), Insecure Direct Object Reference Vulnerability (**).

4. **Lab4: SQL Injection**- Injection attacks are discussed in the OWASP injection module. According to the OWASP authors, injection flaws are very prevalent and are often found in SQL, LDAP, XPath, or NoSQL queries, OS commands, XML parsers, SMTP headers, expression languages, and ORM

queries. They can be easily discovered using automated tools such as scanners and fuzzers. In the exercises prepared for this topic, we mostly focused on SQL-based attacks. SQL injection is an attack that inserts (injects) a malicious part of an SQL query to a database in a loaded request that is created by an application. Virtual laboratories in this topic are based on OWASP A03:2021-Injection and consist of the five exercises described in detail below as: Classic SQL Injection Vulnerability (*), Reading the Database Schema (**), Identification of the Database Server Version (**), Blind SQL Injection Vulnerability (***), Time-Based SQL Injection Vulnerability (***).

5. **Lab5: Cross-Site Scripting (XSS)**-According to OWASP, cross-site scripting (XSS) attacks can be found in around two-thirds of all web applications. Cross-site scripting (XSS) attacks are a type of attack involving injection, where malicious input data (such JavaScripts) are inserted in the HTML code of WWW pages. There are three forms of XSS, usually targeting users' browsers: reflected XSS (injecting code to the HTTP request), stored XSS (injecting code into a data source that provides data for the page), and DOM XSS (used when an application uses JavaScript to dynamically create the page content). Virtual laboratories in this topic are based on OWASP A08:2021—Software and Data Integrity Failures and consist of the seven exercises described in detail below as: Stored XSS Vulnerability (*), Reflected XSS Vulnerability (*), DOM XSS Vulnerability (*), XSS Vulnerability (Other Vector) (**), XSS Vulnerability (Filtering Out Tags) (**), XSS Vulnerability (Improved Tag Filtering) (**), XSS Vulnerability (Input Validation) (***).

6. **Lab6: Handling Data from an Untrusted Source**-- Data coming from external sources (such as data entered by application users) cannot be recognized by the application as trusted; the application should verify their correctness (e.g., format). One of the most common web application security vulnerabilities is an incorrect check of the correctness of the input data from a client or environment. Data that are modified or prepared unexpectedly can be used for application logic abuse attacks, denial of service (a DoS type of attack), or execution of any code after deserialization of the data. In this section, students learn about common security gaps that emerge from incorrect or unimplemented data validation mechanisms. Virtual laboratories in this topic are based on OWASP A09:2021—Security Logging and Monitoring Failures and OWASP A10:2021—Server-Side Request Forgery and consist of 10 exercises as described in detail below as: Reading an Unexpected File (*), Reading an Unexpected File with the Use of PHP Filters (**), Running a Malicious Command by Uploading a File (**), Secure File Upload (***), Remote Reading of an Unexpected File (**), Standard Web Application Firewall (WAF) (***), Protected Files Download (WAF) (****), Insecure Log Browser (*), Secure Log Browser (****), Sending E-mails (****).

7. **Lab7: Processing of Composite Data—** XML external entities (XXE) attacks can cause denial of service, file scans, and remote code execution that undermine the security of the system. Understanding the relationship between XML files, parsing, and weak parsing is imperative to understanding what an XXE attack is and why such an attack can put the system at risk. Virtual laboratories in this topic are based on OWASP A08:2021—Software and Data Integrity Failures and consist of the six exercises described in detail below as: Unprotected Parsing of XML Files (*), Denial-of-Service Attack with the Use of an XML Bomb (*), Unprotected Object Deserialization (*), Protected Parsing of XML Files (**), From Deserialization of the Object to Code Execution on the Server (***), Real Attack on the Framework Using Object Deserialization (****).

8. **Lab8: Configuration Errors--** Security misconfiguration vulnerabilities can occur when a web application component is susceptible to attack due to misconfiguration or an insecure configuration option. Virtual laboratories in this topic are based on OWASPA05:2021—Security Misconfiguration and OWASP A06:2021—Vulnerable and Outdated Components and consist of the six exercises described in detail below as: Publicly Accessible Administration Panel (**), Insecure Database Server Configuration (**), Publicly Accessible Development Server (**), Using Default Passwords (**), Outdated Software with Known Vulnerabilities (**), Publicly Available Backup (**).

9. **Lab9: Cross Site Request Forgery (CSRF)--** The objective of this lab is to help students understand the Cross-Site Request Forgery (CSRF) attack. A CSRF attack involves a victim user, a trusted site, and a malicious site. The victim user holds an active session with a trusted site while visiting a malicious site. The malicious site injects an HTTP request for the trusted site into the victim user session, causing damages.

10. **Lab10: JWT security and session hijacking**

11. **Lab11: Local File Inclusion (LFI) and Remote File Inclusion (RFI).**

Lab Practical Resources:

1. Ksiezopolski, Bogdan, et al. "Teaching a Hands-On CTF-Based Web Application Security Course." *Electronics* 11.21 (2022): 3517.
2. Cross Site Request Forgery (CSRF), Available online: https://seedsecuritylabs.org/Labs_16.04/PDF/Web_CSRF_Elgg.pdf (accessed on 15 January 2023).

NOTE: A student must perform at least ten experiments. Seven experiments should be performed from the above list. Remaining three experiments may either be performed from the above list or designed & set by the concerned institution as per the scope of the syllabus.

PC-CS-CYS-407LA	Cloud Security Lab						
Lecture	**Tutorial**	**Practical**	**Credit**	**Minor Test**	**Practical**	**Total**	**Time**
0	**0**	**2**	**1**	**40**	**60**	**100**	**3 Hours**
Purpose	Understand the cloud deployment and security tools						
Course Outcomes (CO)							
CO1	Learn various cloud deployment tools						
CO2	Learn about Cloud security metrics.						
CO3	Explore threat in cloud services & application.						
CO4	To get the knowledge about work with cloud management Platform						

LIST OF PRACTICALS

1. Installation and configuration of Microsoft Azure/AWS/Cloud Stack environment

2. Implement Service deployment & Usage over cloud.

3. Perform Management actions of cloud resources and prepare report.

4. Using existing cloud characteristics & Service models deploy various services.

5. Perform Cloud Security Management Operations

6. Performance evaluation of services over cloud.

B. Tech Computer Science and Engineering (Cyber Security)
Modified Scheme of Studies/Examination (w.e.f. Session 2023-24)
Semester VIII

S. No.	Course No.	Subject	L: T:P	Hours/ Week	Credits	Examination Schedule				Duration of Exam (Hrs.)
						Major Test	Minor Test	Practical	Total	
1	PC-CS- CYS-402A	Block Chain in Cyber security	3:0:0	3	3	75	25	0	100	3
2	HSS-404A	Entrepreneurship and Start-ups	3:0:0	3	3	75	25	0	100	3
3	OEC	OEC Elective*-III	3:0:0	3	3	75	25	0	100	3
4	PE-III	Elective*-III	2:0:0	2	2	75	25	0	100	3
5	PE-IV	Elective* - IV	2:0:0	2	2	75	25	0	100	3
6	PC-CS- CYS-406LA	Cyber security Block Chain Lab	0:0:2	2	1	0	40	60	100	3
7	PC-CS- CYS-410LA	Project-II	0:0:10	10	5	0	100	100	200	3
8	PC-CS- CYS-412LA	General Fitness & Professional Aptitude	0:0:0	0	0	0	0	100	100	3
		Total		**25**	**19**	**375**	**265**	**260**	**900**	

Code	PE Elective* -III	Code	PE Elective* -IV
PE-CS- CYS- 414A	Penetration Testing	PE-CS- CYS- 422A	Intrusion detection and Prevention
PE-CS- CYS- 416A	Identity and Access Management	PE-CS- CYS- 424A	Introduction to Cyber Crime Investigations
PE-CS- CYS- 420A	Biometric Security	PE-CS- CYS- 426A	Social Networks

Code	OEC Elective*-III
OE-CS- CYS-402	Backup Disaster & Recovery
OE-CS- CYS-404	Cryptographic Fundamentals
OE-CS- CYS-406	Artificial Intelligence
OE-CS- CYS-408	Reasoning, Problem Solving and Robotics
OE-CS- CYS-410	Data Injection

Note:
****The students will choose any two departmental Electives courses and One Open Elective course out of the given elective list in VIII Semester.***

*****Project should be initiated in the beginning of 8th semester, and should be completed by the end of 8th semester with good Report and power-point Presentation etc.***

HSS-404A	Entrepreneurship and Start-ups						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
3	**0**	**0**	**3**	**75**	**25**	**100**	**3 Hour**
Purpose	To expose students to the joys and skills of being an entrepreneur.						
Course Outcomes (CO)							
CO1	To understand the basics of Entrepreneurship.						
CO2	To learn the basics of Creative and Design Thinking.						
CO3	To apply the Business Enterprises.						
CO4	To know about business models.						

Unit I

Introduction to Entrepreneurship, Meaning and concept of entrepreneurship, the history of entrepreneurship development, role of entrepreneurship in economic development, Myths about entrepreneurs, types of entrepreneurs.

Unit II

The skills/ traits required to be an entrepreneur, Creative and Design Thinking, the entrepreneurial decision process, entrepreneurial success stories.

Unit III

Crafting business models and Lean Start-ups: Introduction to business models; Creating value propositions- conventional industry logic, value innovation logic; customer focused innovation; building and analysing business models; Business model canvas, Introduction to lean start-ups, Business Pitching.

Unit IV

Institutions Supporting Small Business Enterprises: Central level institutions. State level institutions. Other agencies. Industry Associations. Class exercise- discussions on current government schemes supporting entrepreneurship and finding out which scheme will most

suit the business plan devised by the student.

Text Books:

- Kuratko, D , Hornsby J.S. (2017) New Venture Management: Entrepreneur's roadmap
- Hisrich, R.D., Manimala, M.J., Peters, M.P., Shepherd, D.A.: Entrepreneurship, Tata McGraw Hill
- Ries, Eric(2011)The lean Start-up: How constant innovation creates radically
- S. Carter and D. Jones-Evans (2012), Enterprise and small business- Principal Practice and Policy, Pearson Education (2006)

PC-CS-CYS-402A	Block Chain in Cyber Security						
L	**T**	**P**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
3	**0**	**0**	**3**	**75**	**25**	**100**	**3 hrs**
Purpose	***Purpose To provide knowledge of various* Blockchain *& Cyber Security***						
Course Outcomes (CO)							
CO 1	*To learn the basics of Blockchain Concepts & Architecture.*						
CO 2	*To explore knowledge of various process of Cyber attacks on blockchain*						
CO 3	To understand the basics of security issues						
CO 4	To implies the basic of solidity and its deployment						

UNIT I- Blockchain and Smart Contract Fundamentals: Introduction to Blockchain, Importance of Blockchain, need of Blockchain, types of blockchain, Decision Tree, Consensus Mechanism

Cryptography, Hashing, and Digital Signatures: Introduction, Hashing, Hash Function Characteristics, Digital Signatures, Data Encryption, Denial of Serviceman-in-The-Middle Attack, System Resiliency, Infrastructure Hardening.

Unit II-Consensus Protocols: Proof of Work, Security Issues in Proof of Work, Proof of Stake, Security Issues in Proof of Stake, Other Consensus Types

Blockchain Vulnerabilities and Attacks: Network and Consensus Security Issues, Smart Contract and Code Security Issues, Wallet and Client Security Issues, Centralization Security Issues, User Security Issues.

Unit-III -Cyber security for Blockchain: *Introduction, CIA Triad, AAA of Security, Non-repudiation, Risk Measurement, Blockchain Governance, Quantum Computing, Smart Contracts.*

Unit-IV-Solidity: Solidity Language Overview, Storage, Memory, and Call Data, Function Selectors, Interacting with EVM Smart Contracts, Compiling and Deploying Contracts

Smart Contract Security Issues: Security Hacks on Ethereum, Common Vulnerabilities and Attacks, Case Study: The DAO Hack, Case Study: The Poly-Network Hack.

Suggested Books:

1) Ashutosh Saxena "Blockchain Technology: Concepts and Applications"
2) Makoto Yano "Blockchain and Crypto Currency
3) Anand Shinde "Introduction to Cyber Security"

OE-CS-CYS-402	Backup Disaster & Recovery						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
3	**0**	**0**	**3**	**75**	**25**	**100**	**3 Hours**
Purpose	Understanding of business continuity and disaster recovery principles.						
Course Outcomes (CO)							
CO1	Strong understanding of business continuity and disaster recovery principles, including conducting business impact analysis, assessing risks, developing policies and procedures, and implementing a plan.						
CO2	Learn to secure data by putting policies and procedures in place, and how to recover and restore their organizations critical data in the aftermath of a disaster.						
CO3	Learn to implement Data Recovery techniques.						

Unit- I

Introduction to Disaster Recovery and Business Continuity: Overview of Disaster Recovery and Business Continuity, Trends in Disaster Recovery and Business Continuity, Understanding Best Practices in Disaster Recovery and Business Continuity, Overview of Business Continuity Management (BCM), Understanding Best Practices and Standards of BCM.

Risk Assessment: Overview of Risk and its Terminology, Understanding Risk Assessment Process, Understanding Best Practices and Standards in Risk Management.

Unit-II

Business Impact Analysis and Business Continuity Plan: Overview of Cost Benefit Analysis (CBA) and Business Impact Analysis (BIA), Understanding Standards of BIA, Understanding How to Perform BIA, Overview of Business Continuity Plan (BCP), Overview of Business Continuity Strategy Design.

Data Backup Strategies: Overview of Data Backup, Understanding RAID Technology, Overview of SAN and NAS, Understanding Types of Data Backup, Understanding Cloud Data and Disaster Recovery, Overview of Infrastructure Technologies, Understanding Data Protection Continuum and Best Practices in Backup.

Unit-III

Data Recovery Strategies: Overview of Data Recovery, Understanding Data Recovery Process and Best Practices, Understanding Virtualization-Based Disaster Recovery, Understanding Best Practices and Standards in Virtualization, Understanding System Recovery, Overview of Centralized and Decentralized Computing, Overview of Centralized Backup, Data Consolidation, and Survivable Storage Systems.

Unit-IV

Disaster Recovery Planning Process: Overview of Disaster Recovery Planning, Understanding Disaster Recovery Planning Process and Methodology.

BCP Testing, Maintenance, and Training: Overview of Business Continuity Plan Testing, Maintaining and Auditing the Business Continuity Plan, Overview of BCP Training Program.

Suggested Books:

- EC-COUNCIL DISASTER RECOVERY PROFESSIONAL. Available online: https://www.eccouncil.org/programs/business-continuity-and-disaster-recovery-training/ (accessed on 16 January 2023).
- Chakraborty, Bapi, and Yashajeet Chowdhury. Introducing Disaster Recovery with Microsoft Azure. Apress, 2020.

OE-CS-CYS-404	Cryptographic Fundamentals						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
3	**0**	**0**	**3**	**75**	**25**	**100**	**3 Hours**
Purpose	To Understand various cryptographic algorithm, public-key cryptosystem, and fundamental ideas of public-key cryptography.						
Course Outcomes (CO)							
CO1	Student will be able to understand basic cryptographic algorithms.						
CO2	Able to understand the fundamental ideas of public-key cryptography.						
CO3	Analyze and compare symmetric-key encryption public-key encryption schemes based on different security models						
CO4	Able to understand the PKI infrastructure.						

Unit-I

Cryptography Concept: Introduction, plain text and cipher text, substitution techniques, transposition techniques, encryption and decryption, symmetric and asymmetric key cryptography, steganography, key range and key size, possible types of attacks Historical Ciphers, Computational Security, Semantic Security, Pseudorandom Generators (PRGs) PRF, PRP and SPRP.

Unit-II

Symmetric key Ciphers: Block Cipher principles, Modes of Operations of Block Ciphers, DES, AES, Stream ciphers.

Cryptographic Hash Functions: MAC, Information-theoretic Secure MAC, Cryptographic Hash Functions, Birthday Attacks on Cryptographic Hash Functions, Applications of Hash Functions, Generic Constructions of Authenticated Encryption Schemes.

Unit-III

Asymmetric key Ciphers: Discrete-Logarithm Problem, Computational Diffie-Hellman Problem, Decisional Diffie-Hellman Problem, Elliptic-Curve Based Cryptography and Public-Key Encryption, El Gamal Encryption Scheme, RSA Assumption, CCA -secure Public-key Hybrid Ciphers Based on Diffie-Hellman Problems and RSA-assumption, Digital Signatures.

Unit-IV

Key Management and Distribution: Symmetric Key Distribution Using Symmetric & Asymmetric Encryption, Distribution of Public Keys, Kerberos, X.509 Authentication Service, Public – Key Infrastructure, overview of SSL/TLS.

Suggested Books:

1. Cryptography and Network Security: Forouzan Mukhopadhyay, Mc Graw Hill, 3rd Edition.
2. Katz and Y. Lindell, Introduction to Modern Cryptography, CRC press, 2020.
3. Cryptography and Network Security - Principles and Practice: William Stallings, Pearson Education, 6th Edition

OE-CS-CYS-406	Artificial Intelligence						
L	**T**	**P**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
3	**0**	**0**	**3**	**75**	**25**	**100**	**3 Hour**
Purpose	The course provides grounding in basic and advanced methods to big data technology and tools.						
Course Outcomes –							
CO1	Understand the basics of the theory and practice of Artificial Intelligence as a discipline and about intelligent agents.						
CO2	Understand search techniques and gaming theory.						
CO3	The student will learn to apply knowledge representation techniques and problem-solving strategies to common AI applications.						
CO4	Student should be aware of techniques used for classification and clustering. Student should be aware of basics of pattern recognition and steps required for it.						

Unit I-INTRODUCTION: Introduction–Definition – Future of Artificial Intelligence – Characteristics of Intelligent Agents– Typical Intelligent Agents – Problem Solving Approach to Typical AI problems.

Unit II-PROBLEM-SOLVING METHODS Problem-solving Methods – Search Strategies- Uninformed – Informed – Heuristics – Local Search Algorithms and Optimization Problems – Searching with Partial Observations – Constraint Satisfaction Problems – Constraint Propagation – Backtracking Search – Game Playing – Optimal Decisions in Games – Alpha – Beta Pruning – Stochastic Games

Unit III- KNOWLEDGE REPRESENTATION First Order Predicate Logic – Prolog Programming – Unification – Forward Chaining-Backward Chaining – Resolution – Knowledge Representation – Ontological Engineering-Categories and Objects – Events – Mental Events and Mental Objects – Reasoning Systems for Categories – Reasoning with Default Information

Unit IV-SOFTWARE AGENTS Architecture for Intelligent Agents – Agent communication – Negotiation and Bargaining – Argumentation among Agents – Trust and Reputation in Multi-agent systems. APPLICATIONS AI applications – Language Models – Information Retrieval- Information Extraction – Natural Language Processing – Machine Translation – Speech Recognition – Robot – Hardware – Perception – Planning – Moving

Text books:

1. S. Russell and P. Norvig, "Artificial Intelligence: A Modern Approach‖, Prentice Hall, Third Edition, 2009.
2. I. Bratko, ―Prolog: Programming for Artificial Intelligence‖, Fourth edition, Addison-Wesley Educational Publishers Inc., 2011.
3. M. Tim Jones, ―Artificial Intelligence: A Systems Approach(Computer Science)‖, Jones and Bartlett Publishers, Inc.; First Edition, 2008
4. Nils J. Nilsson, ―The Quest for Artificial Intelligence‖, Cambridge University Press, 2009.
5. William F. Clocksin and Christopher S. Mellish, ‖ Programming in Prolog: Using the ISO Standard‖, Fifth Edition, Springer, 2003.
6. Gerhard Weiss, ―Multi Agent Systems‖, Second Edition, MIT Press, 2013.

7. David L. Poole and Alan K. Mackworth, ―Artificial Intelligence: Foundations of Computational Agents‖, Cambridge University Press, 2010.

OE-CS- CYS-408	Reasoning, Problem Solving and Robotics						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
3	**0**	**0**	**3**	**75**	**25**	**100**	**3 Hour**
Purpose	This subject provides the basic knowledge about the knowledge representation and robotics						
Course Outcomes (CO)							
CO1	Understanding of identity governance and data governance.						
CO2	Understanding of backward reasoning and search methods.						
CO3	Understanding of basics of robotics and actuating system.						
CO4	Application and understanding of sensors and robotic controls.						

UNIT-1- Solving problems by reasoning: Definition and Importance of Knowledge, Knowledge-Based Systems, And Representation of Knowledge, Knowledge Organization, Knowledge Manipulation, And Acquisition of Knowledge, The reasoning algorithm, Conflict resolution, Explanation of the reasoning. Forward reasoning: The method of forward reasoning, A simple case study of forward reasoning.

UNIT-II-Backward reasoning: Solving problems by reduction, The method of backward reasoning, A simple case study of backward reasoning, Bidirectional reasoning. Search Methods: Depth-first search, Breadth-first search, Hill climbing search, A* search. Contradiction freeness: The notion of contradiction freeness, Testing contradiction freeness, The search problem of contradiction freeness. Completeness: The notion of completeness, Testing completeness, The search problem of completeness. Decomposition of knowledge bases: Strict decomposition, Heuristic decomposition.

UNIT-III-Introduction to Robotics: Classification, Components, Characteristics, Applications. Robotics Kinematics, Position Analysis, Robots as Mechanisms, Matrix Representation, Transformation Matrices, Forward and Inverse Kinematics. Actuators: Characteristics of Actuating Systems, Actuating Devices and Control, Use of Reduction Gears, Comparison Of Hydraulic, Electric, Pneumatic Actuators, Hydraulic Actuators.

UNIT-IV-Sensors: Sensor Characteristics, Description of Different Sensors, Vision Sensors, Force Sensors, Proximity Sensors, Tilt Sensors.

Robot Controls: Point to Point Control, Continuous Path Control, Intelligent Robot, Control System for Robot Joint, Control Actions, Feedback Devices.

Suggested Books:

1. Intelligent Systems and Control: Principles and Applications Paperback – 12 Nov 2009 by Laxmidhar Behera, Indrani Kar by OXFORD.
2. Intelligent Systems and Technologies Methods and Applications by Springer publications.
3. Intelligent Systems - Modeling, Optimization and Control, by Yung C. Shin and Chengying Xu, CRC Press, Taylor & Francis Group, 2009.
4. Saeed B. Niku, Introduction to Robotics Analysis, Application, Pearson Education Asia, 2001.
5. S.R. Deb, Robotics Technology and flexible automation, Tata McGraw-Hill Education., 2009.
6. Fu. K. S., Gonzalez. R. C. & Lee C.S.G., "Robotics control, sensing, vision and intelligence", McGraw Hill Book co, 1987.
7. Craig. J. J. "Introduction to Robotics mechanics and control", Addison- Wesley, 1999.

OE-CS-CYS-410	Data Injection						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
3	**0**	**0**	**3**	**75**	**25**	**100**	**3 Hour**
Purpose	To understand the basic concept of data injection and role of data injection in cyber security						
Course Outcomes (CO)							
CO1	Understand the basic concept of data injection						
CO2	Understand various concept of SQL that are fundamental to data injection						
CO3	Study of Injection vulnerabilities against hacking and web attacks						
CO4	Explore some introductory concepts data injection in different field						

UNIT I-Introduction to data injection, Cyber security, Cyber-attack, Cyber Warfare and cyber terrorism, types of web attacks, Privacy attack, SQL Injection Attacks, web attack forensics, Injection vulnerabilities

UNIT II-Type of Injection SQL Injection, Blind Injection Detection, Cross-Site Scripting, Broken Authentication & Session Management, Insecure Direct Object References, Failure to Restrict URL, Remote Code Execution.

UNIT III-Hacking Web Applications & SQL Injection: Hacking Web Servers, Types of Web Server Vulnerabilities, Attacks against Web Servers, IIS Unicode Exploits, Patch Management Techniques, Web Server Hardening Methods Web Application Vulnerabilities, Objectives of Web Application Hacking.

UNIT IV-SQL Injection and Buffer Overflows: SQL Injection, Steps to Conduct SQL Injection, SQL Server Vulnerabilities, Countermeasures Buffer Overflows, Types of Buffer Overflows and Methods of Detection, Stack-Based Buffer Overflows, Buffer Overflow Mutation Techniques.

Reference Books:

1. SQL Injection Attacks and Defense, 2nd Edition by Justin Clarke, Syngress.
2. SQL Injection Strategies by Ettore Galluccio, Edoardo Caselli, Gabriele Lombari.
3. SQL Hacks by Andrew Cumming, Gordon Russell
4. The Art of Invisibility by Kevin Mitnick.

PE-CS-CYS-414A	Penetration Testing						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
2	**0**	**0**	**2**	**75**	**25**	**100**	**3 Hour**
Purpose	To enable students to learn various computational models, design paradigms of advanced computer architecture, parallelism approaches and techniques for static and dynamic interconnections.						
Course Outcomes (CO)							
CO1	Classify and interpret various paradigms, models and micro-architectural design of advanced computer architecture as well as identify the parallel processing types and levels for achieving optimum scheduling						
CO2	Identify the roles of VLIW & superscalar processors and branch handling techniques for performance improvement						
CO3	Analyze and interpret the basic usage of various MIMD architectures and relative importance of various types of static and dynamic connection networks for realizing efficient networks.						
CO4	Examine the various types of processors and memory hierarchy levels and cache coherence problem including software and hardware-based protocols to achieve better speed and uniformity.						

Unit I*- Penetration Testing phases/Testing Process, types and Techniques, Blue/Red Teaming, Strategies of Testing, Non-Disclosure Agreement Checklist, Phases of hacking, Open-source/proprietary Pentest Methodologies. Pentest Scoping: The mindset of the professional Pen Tester, creating effective pen test scopes and rules of engagement.*

Unit -II*-Recon: Detailed Recon Using the Latest Tools, Mining Search Engine Results, google hacking database, shodan, Information gathering methodologies- Foot printing, Competitive Intelligence DNS Enumerations- Social Engineering attacks, Port Scanning- Network Scanning Vulnerability Scanning - NMAP scanning tool.*

Unit -III *-System Hacking: Password cracking techniques - Key loggers - Escalating privileges - Hiding Files, Steganography technologies and its Countermeasures. Active and passive sniffing- ARP Poisoning, MAC Flooding. SQL Injection - Errorbased, Union-based, Time- based, Blind SQL, SQL Injection Prevention Techniques.*

Unit – IV*-wireless pentest: Wi-Fi Authentication Modes, Bypassing wlan, wep, wps Authentication practically,Attacks on the WLAN Infrastructure, Wi-Fi deauthentication attack, Wireless Hacking Methodology, Wireless Traffic Analysis, packet capturing, aircrack-ng, capturing the handshake,*

cracking the handshake, Wifi hacking prevention,Legal Documentation and Report Writing: legal documents you may encounter as a penetration tester, Statements of Work, Rules of Engagement, Non-Disclosure Agreements, and Master Service Agreements.

Suggested Books:

The hacker playbook:-Practical guide to penetration testing Author: Kim ISBN -10: 149-4932636/ISBN-13: 978-1494932633

PE-CS- CYS- 416A	Identity and Access Management						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
2	**0**	**0**	**2**	**75**	**25**	**100**	**3 Hour**
Purpose							
Course Outcomes (CO)							
CO1	Understanding of fundamentals and frameworks of identity and access management						
CO2	Application and usage of various authentication protocols						
CO3	Study of Injection vulnerabilities against hacking and web attacks						
CO4	Understanding of identity governance and data governance.						

Unit-I

Identity and access management (IAM): framework, key principles, Capability maturity framework, Common challenges and key considerations: Governance, program delivery, sustain compliance, identity lifecycle, control access, operations. Identity and access intelligence, peer group, outlier analysis, role analysis, resource allocation and analysis, risk and fraud systems integration, kerberos, biometrics, Okta platform, security concepts: job rotation, least privileges, separation of duty.

Cloud based IAM, deployment models, service models, security and risk management. Access request, approval and provisioning: system overview, key components, data management, authentication, authentication implementation approaches, authorization, logging and monitoring, access review and certification process.

Unit-II

LDAP: Basics, Configuration, Managing data, operational consideration. SAML: assertions, protocols, profiles, OAuth: roles, tokens, grants. OpenID connect, proxy: load balancing, access control and security, rate limiting, Caching and compression, telemetry, monetization, API v Web proxies, open-source web proxies. Strong Authentication: OTP, HOTP, TOTP, mutual SSL/TLS, FIDO, W3C web authentication and CTAP.

Unit-III

Privileged Access Management (PAM), Privileged Account, Privileged Account Monitoring, PAM components: credential management, access management, session management, logging, security, reporting, Application whitelisting. Types of access control models, RBAC model, access management life cycle, RBAC implementation considerations. Future of identity and access management

Unit-IV

Identity Governance and Administration (IGA), User Onboarding, User Termination & Role changes, Access control models, Access validation & certification, Segregation of Duties, Auditing and Reporting, Identity lifecycle management, cross domain identity management.

Data Governance and Protection, data types, intellectual property, data classification, industry and local laws & regulations, Data type management & monitoring, security policy framework, data breach and incident response process, notifiable data breaches.

Suggested Books:

1. Identity and Access Management by Ertem Osmanoglu, Syngress, 2013.
2. Securing the Perimeter: Deploying identity and access management with free open source software by Michael Schwartz, Maciej Machulak, Apress, 2018.
3. Keycloak - Identity and Access Management for Modern Applications: Harness the power of Keycloak, OpenID Connect, and OAuth 2.0 protocols to secure applications by Stian thorgersen, Packt publishing ltd, 2021.
4. Focus on IAM (Identity and Access Management): CSFs, metrics, checklists, best practices, and guidelines for defining IAM processes and implementing IAM solutions by Kiran Kumar Pabbathi, ServiceManagers.org,2014.
5. Digital Identity and Access Management: Technologies and Frameworks (Premier Reference Source) 1st Edition by Raj Sharman, Sanjukta Das Smith, Manish Gupta.

PE-CS-CYS-420A	Biometric Security						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
2	**0**	**0**	**2**	**75**	**25**	**100**	**3 Hour**
Purpose	To understand the physical security methods and mechanism.						
Course Outcomes (CO)							
CO1	Identify the various Biometric technologies.						
CO2	Design of biometric recognition for the organization.						
CO3	Develop simple applications for privacy.						
CO4	Understand the need of biometric in the society						

UNIT I INTRODUCTION: Person Recognition – Biometric systems –Biometric functionalities: verification, identification – Biometric systems errors - The design cycle of biometric systems – Applications of Biometric systems – Security and privacy issues.

UNIT II FINGER PRINT AND FACIAL RECOGNITION: FINGERPRINT: Introduction – Friction ridge pattern- finger print acquisition: sensing techniques, image quality –Feature Extraction –matching – indexing. FACE RECOGNITION: Introduction –Image acquisition: 2D sensors ,3D sensors- Face detection-Feature extraction -matching.

UNIT III IRIS AND OTHER TRAITS: Design of an IRIS recognition system-IRIS segmentation-normalization – encoding and matching IRIS quality –performance evaluation –other traits- ear detection – ear recognition –gait feature extraction and matching –challenges- hand geometry –soft biometrics.

UNIT IV BEHAVIORAL BIOMETRICS: Introduction –Features- classification of behavioral biometrics – properties of behavioral biometrics – signature –keystroke dynamics –voice- merits –demerits –applications-error sources-types –open issues –future trends.

UNIT V APPLICATIONS AND TRENDS: Application areas: surveillance applications- personal applications –design and deployment -user system interaction-operational processes – architecture – application development –design validation-disaster recovery plan-maintenance-privacy concerns.

TEXT / REFERENCE BOOKS:

1. James wayman, Anil k. Jain ,Arun A. Ross ,Karthik Nandakumar, ―Introduction to Biometrics‖, Springer, 2011

2. John Vacca "Biometrics Technologies and Verification Systems" Elsevier 2007

3. James Wayman, Anil Jain, David Maltoni, DasioMaio(Eds) "Biometrics Systems Technology", Design and Performance Evalution. Springer

4. Khalid saeed with Marcin Adamski, Tapalina Bhattasali, Mohammed K. Nammous, Piotr panasiuk, mariusz Rybnik and Soharab H.Sgaikh, ―New Directions in Behavioral Biometrics, CRC Press

5. Paul Reid "Biometrics for Network Security "Person Education 2004

6. Shimon K. Modi, Biometrics in Identity Management :concepts to applications‖, Artech House 2011.

PE-CS-CYS- 422A	Intrusion Detection and Prevention						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
2	**0**	**0**	**2**	**75**	**25**	**100**	**3 Hours**
Purpose	To understand the intrusion detection and prevention technologies and various types of network behaviour analysis.						
Course Outcomes (CO)							
CO 1	To understand the intrusion detection and prevention technologies, various types of network behaviour analysis.						
CO 2	To understand the honeypots, multiple IDS methods, tools to analyse various types of attacks like wireless attacks and their detection.						
CO 3	To understand the attack source and provides practical knowledge for dealing with intrusions in real world applications.						

Unit-1

Introduction to IDPS: Introduction of Intrusion detection and Prevention Systems **(**IDPS), Components and Architecture Implementation, Uses of IDPS Technologies, Key Functions, Common Detection Methodologies-- Signature, Anomaly and Stateful Protocol Analysis, Types of IDPS Technologies.

Host and Network IDPS: Application, Transport, Network and Hardware Layer attacks, Sniffing Network Traffic, Replay Attacks, Command Injection, Internet Control Message Protocol Redirect, DDoS, Dangers and defences with Man-in the Middle, Secure Socket Layer attacks, DNS Spoofing, Defence- in-Depth Approach, Port Security, Use Encrypted Protocols.

Unit-2

Network Behaviour Analysis: Components and Architecture Typical, Network Architecture, Sensor Locations.
Honeypots: Honeynets- Gen I, II and III, Detecting the Attack - Intrusion Detection, Network Traffic Capture, Monitoring on the box, Setting up the Realistic Environment, OpenCanary, Cowrie honeypots deployment.

Unit-3

Working with SNORT IDS: Introduction to Snort, Snort Alert Modes and Format, Working with Snort Rules, Rule Headers, Rule Options, The Snort Configuration File etc, Plugins, Pre-processors and Output Modules, Using Snort with MySQL.

Multiple IDPS Technologies: Need for multiple IDPS Technologies, Integrating Different IDPS Technologies - Direct and Indirect, Firewalls, Routers and Honeypots, IPS using IP Trace back - Probabilistic and Deterministic Packet Marking, Marking.

Unit-4

Wireless IDPS: Exception WLAN Standards, WLAN Components, Threats against WLANs, 802.11 Wireless Infrastructure Attacks, WEP Attacks, Wireless Client Attacks, Bluetooth Attacks, Cell phones, Personal Digital Assistance and Other Hybrid Devices Attack Detection, Jailbreaking.

Suggested Books:

1. Shui Yu, Distributed Denial of Service Attack and Defense, Springer, 2014.
2. Bradd Lhotsky, OOSEC Host based Intrusion detection, PACKT Publication, 2013.
3. Sandeep Kumar Shukla, Manindra Agrawal, Cyber Security in India, Springer, 2020.

Note: The Examiner will be given the question paper template and will have to set the question paper according to the template provided along with the syllabus.

PE-CS-CYS-424A	Introduction to Cyber Crime Investigations						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
2	**0**	**0**	**2**	**75**	**25**	**100**	**3 Hours**
Purpose	1. To learn the basics of cyber crime Investigations. 2. To learn about the different digital forensic systems and services 3. To learn about file recovery using various tools 4. To learn about processing the crime scene and preserving digital evidence						
Course Outcomes (CO)							
CO 1	Describe what a digital investigation is, the sources of digital evidence, and the limitations of Forensics.						
CO 2	Describe the legal requirements for use of seized data.						
CO 3	Conduct data collection on backup drives.						
CO 4	Recover data based on a given search term from an imaged system.						

Unit-I

Introduction: Understanding the need of Computer Forensics, Definitions, **Computer Hardware:** Analysis of sources for digital evidence, Digital Media, Hard disk basics, mobile phones, **Forensic Tools:** Forensic hardware, Hardware write/blockers, Hard drive acquisitions, Processing the scene, **Files and File Systems:** Windows file systems, Forensic file images, metadata, File signatures.

Unit-II

Forensic software: Different software packages, Basic search queries, ASCII, UNICODE, Regular expressions, viewing and managing keywords and cases, Encryption, password protection, Password recovery tools, **Physical evidence**: fingerprints or other evidence on machines, keyboards, **Forensic Reports:** Proper report writing, Explaining forensics to the uneducated

Unit–III

Email analysis: IP tracking, Tracking and analysis of emails, Webmail, POP, IMAP, **File signature analysis:** File signatures, File extensions, detecting file manipulation, **Hash Analysis:** Hashing files, Hash libraries, **Window Artifacts:** My documents, recycle bin, Installed programs, Windows XP vs. Windows 7, **File Systems:** FAT/NTFS file Systems, Parsing FAT/NTFS file systems, Prefetch and SuperFetch, Shortcuts and Jumplists, **Adversary and Malware hunting:** Malware detection, Malware analysis

Unit-IV

Memory Forensics: Memory acquisition, Memory analysis, memory analysis tools, Advanced Recycle bin, Server Logs, google forensics, **Anti-Forensics Detection:** detection methodologies, Volume shadow copy, ESE databases, Advanced Registry, Thumbnail cache, **Computer crime and legal issues:** Privacy issues, Intellectual property, **Incident Response:** Threat and Adversary Intelligence, Financial crime analysis, **Live/Online Forensics:** Live Digital Forensics Investigation, **Tools:** BitTorrent, Sleuthkit toolset, Windows Forensics Toolchest

Suggested Books:

- Parasram, Shiva VN. Digital Forensics with Kali Linux: Perform data acquisition, data recovery, network forensics, and malware analysis with Kali Linux 2019. x. Packt Publishing Ltd, 2020.
- Bill Nelson, Amelia Philips, Christopher Steuart, Guide to Computer Forensics and Investigations, Fifth Edition, Cengage Learning,2016.
- Luttgens, Jason T., Matthew Pepe, and Kevin Mandia. Incident response & computer forensics. McGraw-Hill Education Group, 2014.

Note: The Examiner will be given the question paper template and will have to set the question paper according to the template provided along with the syllabus.

PE-CS-CYS- 426A	Social Networks						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
2	**0**	**0**	**2**	**75**	**25**	**100**	**3 Hour**
Purpose	Students will be able to use social networks for business and personal use, conducting social network analysis, social network developer tools and social network concepts for solving real-world issues.						
Course Outcomes (CO)							
CO1	Demonstrate proficiency in the use of social networks for business and personal use						
CO2	Demonstrate proficiency in the use of social network analysis concepts and techniques.						
CO3	Demonstrate proficiency in the use of social network developer tools.						
CO4	Examine the various types of processors and demonstrate proficiency in the use of social network concepts for solving real world issues.						

UNIT 1 INTRODUCTION

Introduction to Semantic Web: Limitations of current Web - Development of Semantic Web - Emergence of the Social Web - Social Network analysis: Development of Social Network Analysis - Key concepts and measures in network analysis - Electronic sources for network analysis: Electronic discussion networks, Blogs and online communities - Web-based networks - Applications of Social Network Analysis.

UNIT 2 MODELLING, AGGREGATING AND KNOWLEDGE REPRESENTATION

Ontology and their role in the Semantic Web: Ontology-based knowledge Representation - Ontology languages for the Semantic Web: Resource Description Framework - Web Ontology Language - Modeling and aggregating social network data: State-of-the-art in network data representation - Ontological representation of social individuals - Ontological representation of social relationships - Aggregating and reasoning with social network data - Advanced representations.

UNIT 3 EXTRACTION AND MINING COMMUNITIES IN WEB SOCIAL NETWORKS

Extracting evolution of Web Community from a Series of Web Archive - Detecting communities in social networks - Definition of community - Evaluating communities - Methods for community detection and mining - Applications of community mining algorithms - Tools for detecting communities social network infrastructures and communities - Decentralized online social networks.

UNIT 4 PREDICTING HUMAN BEHAVIOUR AND PRIVACY ISSUES

Understanding and predicting human behavior for social communities - User data management - Inference and Distribution - Enabling new human experiences - Reality mining - Context - Awareness - Privacy in online social networks - Trust in online environment - Trust models based on subjective logic - Trust network analysis.

TEXT BOOKS:

1. Peter Mika, Social Networks and the Semantic Web‖, First Edition, Springer 2007.
2. Borko Furht, Handbook of Social Network Technologies and Applications, 1st Edition, Springer, 2010.

REFERENCES

1. Guandong Xu ,Yanchun Zhang and Lin Li, Web Mining and Social Networking Techniques and applications‖, First Edition, Springer, 2011.
2. Dion Goh and Schubert Foo, Social information Retrieval Systems: Emerging Technologies and Applications for Searching the Web Effectively‖, IGI Global Snippet, 2008.

PC-CS-CYS-406LA	Cyber Security Block Chain Lab						
Lecture	**Tutorial**	**Practical**	**Credit**	**Minor Test**	**Practical**	**Total**	**Time**
0	**0**	**2**	**1**	**40**	**60**	**100**	**3 Hrs.**
Purpose	To implement the concepts of Blockchain Network in Cyber security.						
Course Outcomes-Attend of the course students will be able to:							
CO1	Implement solidity programming language.						
CO2	Implement various process of blockchain network.						
CO3	Implement meta mask to execute the smart contract.						
CO4	Implement various type of smart contract and its deployment.						

1) Write a program in remix that calculate the prime number in solidity.

2) Write a program to implement various hash function used in cryptography Technique.

3) Deposit some Ether in your MetaMask accounts.

4) Create several accounts and make some transactions between these accounts on Rinkeby Network.

5) Test some properties of cryptographic hashing like small change in input results in big change in output.

6) Write a smart contract in remix that execute different data types in solidity.

7) Write a smart contract in remix that execute different Error handling functions in solidity.

8) Write a smart contract in remix that execute concept of inheritance in solidity.

9) Write a smart contract in remix that execute different loops in solidity.

10) Write a program in remix that execute different events in solidity.