RAMAIAH
Institute of Technology

CURRICULUM

Academic year 2025 – 2026

V & VI SEMESTER

B.E.

Computer Science and Engineering

(Cyber Security)

Batch - 2023

RAMAIAH INSTITUTE OF TECHNOLOGY

(Autonomous Institute, Affiliated to VTU)
(Approved by AICTE, New Delhi & Govt. of Karnataka)
Accredited by NBA & NAAC with A Grade

About the Institute:

Dr. M. S. Ramaiah a philanthropist, founded 'Gokula Education Foundation' in 1962 with an objective of serving the society. M S Ramaiah Institute of Technology (MSRIT) was established under the aegis of this foundation in the same year, creating a landmark in technical education in India. MSRIT offers 18 UG programs and 15 PG programs. All these programs are approved by AICTE. All eligible UG and PG programs are accredited by National Board of Accreditation (NBA). The institute is accredited with **'A^+' grade by NAAC in March 2021** for 5 years. University Grants Commission (UGC) & Visvesvaraya Technological University (VTU) have conferred Autonomous Status to MSRIT for both UG and PG Programs since 2007. The institute has also been conferred autonomous status for Ph.D. program since 2021. The institute is a participant to the Technical Education Quality Improvement Program (TEQIP), an initiative of the Government of India. The institute has 380 competent faculty out of which 70% are doctorates. Some of the distinguished features of MSRIT are: State of the art laboratories, individual computing facility for all faculty members, all research departments active with sponsored funded projects and more than 300 scholars pursuing Ph.D. To promote research culture, the institute has established Centre of Excellence for Imaging Technologies, Centre for Advanced Materials Technology, Centre for Antennas and Radio Frequency systems (CARFS), Center for Cyber Physical Systems, Schneider Centre of Excellence & Centre for Bio and Energy Materials Innovation.

The Entrepreneurship Development Cell (EDC) and "Ramaiah Evolute" have been set up on campus to incubate startups. MSRIT has a strong Placement and Training department with a committed team, a good Mentoring/Proctorial system, a fully equipped Sports department, large air-conditioned library with good collection of book volumes and subscription to International and National Journals. The Digital Library subscribes to online e-journals from Elsevier Science Direct, IEEE, Taylor & Francis, Springer Link, etc. The Institute is a member of DELNET, CMTI and VTU E-Library Consortium. The Institute has a modern auditorium, recording studio, and several hi-tech conference halls with video conferencing facilities. The institute has excellent hostel facilities for boys and girls. MSRIT Alumni have distinguished themselves by occupying high positions in India and abroad and are in touch with the institute through an active Alumni Association.

As per the National Institutional Ranking Framework (NIRF), MoE, Government of India, M S Ramaiah Institute of Technology has achieved 75th rank among 1584 top Engineering Institutions & 31st Rank among 131 Schools of Architecture in India for the year 2025.

About the Department

The Department offers Bachelor of Engineering (B. E) in Computer Science and Engineering (Cyber Security). The department is started in the year 2021 with an intake of 60 each. Currently intake for B.E. in Computer Science and Engineering (Cyber Security) is 129. The department has experienced faculty members with the doctoral degree. The faculty members of the department are actively involved in the research activities and publishing their research findings in reputed International Journals/Conferences/Book Chapters. The faculty members have authored books with premiere publishing agencies like Springer, Taylor & Francis.

The Department has state-of-the-art laboratories and classroom facilities. The department regularly conducts Bootcamps, Technical Seminars, Workshops, Faculty Development Programs and Hackathons. The department encourages the students to participate in cocurricular and extracurricular activities. The department has established strong collaborations with Industries and premier peer Institutes to design the curriculum to meet the global standards in the domains of Cyber Security.The department is partnering with Ramaiah Medical and Dental College to work on projects which has societal impact. The department is having collaborations with Industries like SAP Labs, Unisys, IBM, HPE, Samsung, Microsoft, GE Healthcare, Adobe, Thomson Reuters, Yubi, JP Morgan, Intellytix etc. to support Internships, Projects, Curriculum upgradation, Guest Lectures, and Industry Visits..

VISION OF THE INSTITUTE

To be an Institution of International Eminence, renowned for imparting quality technical education, cutting edge research and innovation to meet global socio-economic needs

MISSION OF THE INSTITUTE

MSRIT shall meet the global socio-economic needs through

1. Imparting quality technical education by nurturing a conducive learning environment through continuous improvement and customization
2. Establishing research clusters in emerging areas in collaboration with globally reputed organizations
3. Establishing innovative skills development, techno-entrepreneurial activities and consultancy for socio-economic needs

QUALITY POLICY

We at M. S. Ramaiah Institute of Technology strive to deliver comprehensive, continually enhanced, global quality technical and management education through an established Quality Management System complemented by the synergistic interaction of the stake holders concerned

VISION OF THE DEPARTMENT

To provide quality education, inculcate professionalism, and enhance problem solving and coding, innovative design skills in Computer Science and Engineering especially in the domain of AI & ML and Cyber Security with a focus to produce professionally competent and socially sensitive engineers capable of working in a global environment.

MISSION OF THE DEPARTMENT

To pursue excellence in Academics, Research and Innovation by:

1. Enabling creative and dynamic learning environments to impart quality technical education through continuously improving curriculum and pedagogy techniques.
2. Collaborating with the industry, academia and society for strengthening design thinking, research, innovation, and entrepreneurship ecosystem.
3. Encouraging extra and co-curricular activities to nurture the leadership qualities with a sense of commitment and accountability and inculcate values and ethics.

PROGRAM EDUCATIONAL OBJECTIVES (PEOs):

A B.E in Computer Science & Engineering (Cyber Security) graduate of Ramaiah Institute of Technology:

PEO1: Excel in professional career by acquiring knowledge in basic sciences and Computer Science and Engineering, Cyber Security and Data science principles and contribute to the profession as an excellent employee, or as an entrepreneur.

PEO2: Capable of pursuing higher education and research.

PEO3: Adapt to technological advancements in multidisciplinary environments by engaging in lifelong learning with leadership qualities, professional ethics and soft skills.

PROGRAM OUTCOMES (POs):

The Outcomes of the Bachelor of Engineering in Computer Science & Engineering (Cyber Security) Programme are as follows:

PO1: Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

PO2: Problem analysis: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

PO3: Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

PO4: Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

PO5: Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations.

PO6: The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

PO7: Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

PO8: Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

PO9: Individual and teamwork: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

PO10: Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

PO11: Project management and finance: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one‘s own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

PO12: Life-long learning: Recognize the need for and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

PROGRAM SPECIFIC OUTCOMES (PSOs):

PSO1: Ability to understand and identify problems/opportunities where CSE, Cyber Security concepts can be applied and to identify the right AI and ML techniques in such contexts.

PSO2: Ability to perform the data engineering, designing, developing and testing the Cyber Security solutions that include both hardware and software.

PSO3: Ability to be aware of technical solutions that are following ethical aspects aligning with social responsibilities both at designing and developmental phases of applications.

Semester wise Credit Breakdown for B.E Degree Curriculum

Batch 2023-2027

Semester / Course Category	First	Second	Third	Fourth	Fifth	Sixth	Seventh	Eighth	Total Credits
Basic Sciences (BSC)	08	08	03	03	--	--	--	--	22
Engineering Sciences (ESC)	09	08	--	--	--	--	--	--	17
Humanities, Social Sciences and Management (HSMC)	02	02	--	--	03	03	--	--	10
Ability Enhancement Course (AEC)	01	02	01	01	01	--	--	--	06
Universal Human Values (UHV)	--	--	02	--	--	--	--	--	02
Professional Core Course (PCC)	--	--	11	12	12	06	04	--	45
Integrated Professional Core Course (IPCC)	--	--	04	04	03	--	04	--	15
Professional Elective Course (PEC)	--	--	--	--	03	06	03	--	12
Institutional Open Elective Course (IOE)	--	--	--	--	--	03	03	--	06
Internship (INT)	--	--	--	--	--	--	--	05	05
Mini Project / Project Work (PW)	--	--	--	--	--	04	--	13	17
Skill Enhancement Course (SDC)			--	--		01	02		03
Non Credit Mandatory Course (NCMC)	--	--	--	--	Yes	--	--	Yes	--
Total Credits	20	20	21	20	22	23	16	18	160

SCHEME OF TEACHING V SEMESTER

Sl. No.	Subject Code	Subject	Teaching Department	Category	Credits				Total contact hours /week
					L	T	P	Total	
1	CY51	Foundations to AI & ML	CSE(AIML)	IPCC	2	1	0	3	4
2	CY52	Advanced Computer Networks	CSE(AIML)	PCC	2	0	1	3	4
3	CY53	Cryptography and Network Security	CSE(AIML)	PCC	4	0	0	4	4
4	CY54	Software Engineering	CSE(AIML)	PCC	3	0	0	3	3
5	CYE55x	Program Elective Course – 1	CSE(AIML)	PEC	3	0	0	3	3
6	CYL56	Application Development using Java Laboratory	CSE(AIML)	PCC	0	0	1	1	2
7	CYL57	Cryptography and Network Security Laboratory	CSE(AIML)	PCC	0	0	1	1	2
8	AL58	Research Methodology & Intellectual Property Rights	CSE(AIML)	HSMC	3	0	0	3	3
9	CYAEC59	Ability Enhancement Course – V DevOps	Any Dept.	AEC	1	0	0	1	1
				Total	18	1	3	**22**	**26**
10	HS510	Environmental Studies *	Humanities	NCMC	0	0	0	0	1

PROGRAM ELECTIVE – 1							
SL. NO.	COURSE CODE	COURSE NAME	Credits				Total contact hours /week
			L	T	P	Total	
1.	CYE551	Secure Coding using C/C++	3	0	0	3	3
2.	CYE552	Cyber Warfare	3	0	0	3	3
3.	CYE553	Identity Access Management	3	0	0	3	3

4.	CYE554	Block Chain Technology	3	0	0	3	3
5.	CYE555	Internet of Things	3	0	0	3	3

*** Environmental Studies is under the category of NCMC, 1-hour teaching per week has to be allocated in the time table.**

Nomenclature: IPCC: Integrated Professional Core Course**, PCC:** Professional Core Course**, HSMC:** Humanity and Social Science & Management Courses**, PEC:** Professional Elective Courses**, AEC–**Ability Enhancement Courses,
NCMC: Non-credit Mandatory Course

L –Lecture, T – Tutorial, P- Practical/ Drawing

Note: CIE55x, where x=1,2,3,4,5

Integrated Professional Core Course (IPCC): Refers to Professional Theory Core Course Integrated with practical of the same course. Credit for IPCC is 03 and its Teaching–Learning hours (L: T: P) can be considered as (2: 0: 1). The theory part of the IPCC shall be evaluated both by CIE and SEE. The practical part shall be evaluated only by CIE (no SEE). However, questions from the practical part of IPCC can be included in the SEE question paper.

Professional Elective Courses: A professional elective (PEC) course is intended to enhance the depth and breadth of educational experience in Engineering and Technology curriculum. Multidisciplinary courses that are added supplement the latest trend and advanced technology in the selected stream of engineering. Each group will provide an option to select one course out of five courses. The minimum student‘s strength for offering professional electives is 10. However, this conditional shall not be applicable to cases where the admission to the program is less than 10.

Innovation/ Societal/ Entrepreneurship based Internship: At the End of fourth Semester four - weeks Summer Internship Shall Be Carried Out – Based On industrial/Govt./NGO/MSME/Rural Internship/Innovation/Entrepreneurship. Credited in fifth Semester. All the students admitted shall have to undergo mandatory internship of 04 weeks during the vacation of IV semester. A Viva-Voce examination shall be conducted during VI semester and the prescribed credit shall be included in VI semester. Internship shall be considered as a head of passing and shall be considered for the award of degree. Those, who do not take-up/complete the internship shall be declared fail and shall have to complete during subsequent examination after satisfying the internship requirements.

AICTE Activity Points to be earned by students admitted to BE program (For more details refer to Chapter 6, AICTE, Activity Point Program, Model Internship Guidelines):

Every regular student, who is admitted to the 4-year degree program, is required to earn 100 activity points in addition to the total credits earned for the program. Students entering 4 years‘ degree program through lateral entry are required to earn 75 activity points in addition to the total credits earned for the program. The activity points earned by the student shall be reflected on the students 8^{th} semester grade card. The activities to earn the points can be spread over the duration of the course. However, minimum prescribed duration should be fulfilled. Activity points (non-credit) have no effect on SGPA/CGPA and shall not be considered for vertical progression. In case student fail to earn the prescribed activity points; 8^{th} semester grade card shall be issued only after earning the required activity Points. Students shall be eligible for the award of degree only after the release of the 8^{th} semester grade card.

The Non-Credit Mandatory Course The students shall attend classes for the course during the semester and complete all formalities of attendance and CIE. In case, any student fails to secure the minimum 40% of the prescribed CIE marks, he/she shall be deemed to have secured **„F‟** grade. In such a case, the student has to fulfil the requirements during subsequent semester/s to appear for CIE. This Course shall not be considered for vertical progression, but completion of the course shall be mandatory for the award of the degree.

SCHEME OF TEACHING VI SEMESTER

Sl. No.	Subject Code	Subject	Teaching Department	Category	Credits				Total contact hours /week
					L	T	P	Total	
1	AL61	Management & Entrepreneurship	CSE(CS)	HSMC	3	0	0	3	3
2	CY62	Cyber Security attacks and Defense Strategies	CSE(CS)	PCC	3	1	0	4	5
3	CYE63x	Program Elective Course – 2	CSE(CS)	PEC	3	0	0	3	3
4	CYE64x	Program Elective Course – 3	CSE(CS)	PEC	3	0	0	3	3
5	CYL65	Vulnerability Assessment and Penetration Testing Laboratory	CSE(CS)	PCC	0	0	1	1	2
6	CYL66	Cyber Shield Laboratory	CSE(CS)	PCC	0	0	1	1	2
7	CYOE0x*	Institutional open elective	Any Dept.	IOE	3	0	0	3	3
8	CYP67	Mini Project	CSE(CS)	PW	0	0	4	4	-
9	CYP68	Technical Skill Enhancement Course	CSE(CS)	INT	0	1	0	1	2
Total					**15**	**2**	**6**	**23**	**25**

PROGRAM ELECTIVE – 2								
SL.NO	COURSE CODE	COURSE NAME	Credits				Total contact hours /week
			L	T	P	Total	
1	CYE631	Malware Analysis	3	0	0	3	3
2	CYE632	Cyber Threat Intelligence	3	0	0	3	3

3	CYE633	Secure Software Development Life Cycle	3	0	0	3	3
4	CYE634	Security Testing	3	0	0	3	3
5	CYE635	Privacy Management	3	0	0	3	3

PROGRAM ELECTIVE – 3							
SL.NO	**COURSE CODE**	**COURSE NAME**	**Credits**				**Total contact hours /week**
			L	**T**	**P**	**Total**	
1	CYE641	Deep Learning	3	0	0	3	3
2	CYE642	Big Data Systems	3	0	0	3	3
3	CYE643	Parallel Computing	3	0	0	3	3
4	CYE644	Full Stack Development	3	0	0	3	3
5	CYE645	Quantum Computing	3	0	0	3	3

OPEN ELECTIVE – 1 for other Departments							
SL.NO	**COURSE CODE**	**COURSE NAME**	**Credits**				**Total contact hours /week**
			L	**T**	**P**	**Total**	
1	CIOE01	Web App Development	3	0	0	3	3
2	CIOE02	Python Programming	3	0	0	3	3
3	CIOE03	Data Base Management Systems	3	0	0	3	3
4	CIOE04	Programming in JAVA	3	0	0	3	3
5	CIOE05	Introduction to Artificial Intelligence	3	0	0	3	3

Nomenclature, PCC: Professional Core Course**, PEC:** Professional Elective Courses, **IOE:** Institutional Open Elective, **PW:** Mini Project, **INT –** Internship

L –Lecture, T – Tutorial, P- Practical/ Drawing

Note: CIE63x , where x=1,2,3,4,5

CIE64x , where x=1,2,3,4,5

CIOE0x*, where x=1,2,..,… continued from previous

L –Lecture, T – Tutorial, P- Practical/ Drawing/ Project work

Professional Elective Courses: A professional elective (PEC) course is intended to enhance the depth and breadth of educational experience in Engineering and Technology curriculum. Multidisciplinary courses that are added supplement the latest trend and advanced technology in the selected stream of engineering. Each group will provide an option to select one course out of five courses. The minimum student‘s strength for offering professional electives is 10. However, this conditional shall not be applicable to cases where the admission to the program is less than 10.

Institutional Open Elective Courses:

Students belonging to a particular stream of Engineering and Technology are not entitled for the open electives offered by their parent department. However, they can take an elective offered by other departments, provided they satisfy the prerequisite condition, if any. Registration to open electives shall be documented under the guidance of the Program Coordinator/ Advisor/Mentor.

Selection of an open elective shall not be allowed if,

1. The candidate has studied the same course during the previous semesters of the program.
2. The syllabus content of open electives is similar to that of the Departmental core courses or professional electives.
3. A similar course, under any category, is prescribed in the higher semesters of the program.
4. The minimum students ‘strength for offering open electives is 10. However, this condition shall not be applicable to cases where the admission to the program is less than 10.

Mini-project work: Mini Project is a laboratory-oriented course which will provide a platform to students to enhance their practical knowledge and skills by the development of small systems/applications.

Based on the ability/abilities of the student/s and recommendations of the mentor, a single discipline or a multidisciplinary Mini- project can be assigned to an individual student or to a group having not more than 4 students.

CIE procedure for Mini-project:

(i) Single discipline: The CIE marks shall be awarded by a committee consisting of the Head of the concerned Department and two faculty members of the Department, one of them being the Guide. The CIE marks awarded for the Mini-project work shall be based on the evaluation of project report, project presentation skill, and question and answer session as per the rubrics defined by the department.

(ii) Interdisciplinary: Continuous Internal Evaluation shall be group-wise at the college level with the participation of all the guides of the project. The CIE marks awarded for the Mini-project, shall be based on the evaluation of project report, project presentation skill, and question and answer session as per the rubrics defined by the parent department.

SEE component for Mini-Project: SEE will be conducted by the two examiners appointed by the Institute. SEE marks awarded for the mini project shall be based on the evaluation of project work report, project presentation skill and question and answer session.

Research/Industrial Internship - At the end of sixth / seventh semester (in two cycles to accommodate all the students of the) Research/Industrial Internship shall be carried out – Based on Industrial/Govt./NGO/MSME/Rural Internship/Innovation/Entrepreneurship. All the students admitted shall have to undergo mandatory internship of 24 weeks during the vacation of VI/VII semesters. A Viva-Voce examination shall be conducted during VII semester and the prescribed credit shall be included in VII semester. Internship shall be considered as a head of passing and shall be considered for the award of degree. Those, who do not take-up/complete the internship shall be declared fail and shall have to complete during subsequent examination after satisfying the internship requirements.

Research internship Students have to take up research internship at Centers of Excellence (CoE) / Study Centers established in the same institute and /or out of the institute at reputed research organization / Institutes. Research internship is basically intended to give you the flavor of current research going on in a particular topic/s. The internships serve this purpose. They help students get familiarized with the field, the skill needed the effort amount and kind of effort required for carrying out research in that field.

Industry internships: Is an extended period of work experience undertaken by /Institute students looking to supplement their degree with professional development. The students are allowed to prepare themselves for the workplace and develop practical skills as well as academic ones. It also helps them learn to overcome unexpected obstacles and successfully navigate organizations, perspectives, and cultures. Dealing with "unexpected contingencies" helps students recognize, appreciate, and adapt to organization realities by tempering knowledge with practical constraints.

AICTE Activity Points to be earned by students admitted to BE program (For more details refer to Chapter 6, AICTE, Activity Point Program, Model Internship Guidelines):

Every regular student, who is admitted to the 4-year degree program, is required to earn 100 activity points in addition to the total credits earned for the program. Students entering 4 years' degree program through lateral entry are required to earn 75 activity points in addition to the total credits earned for the program. The activity points earned by the student shall be reflected on the students 8th semester grade card. The activities to earn the points can be spread over the duration of the course. However, minimum prescribed duration should be fulfilled. Activity points (non-credit) have no effect on SGPA/CGPA and shall not be considered for vertical progression. In case student fail to earn the prescribed activity points; 8th semester grade card shall be issued only after earning the required activity Points. Students shall be eligible for the award of degree only after the release of the 8th semester grade card.

FOUNDATIONS OF AI & ML	
Course Code: CY51	**Credits: 2:1:0**
Prerequisite: Nil	**Contact Hours: 28L+14T**
Course Coordinator: Dr. Naveen N C	

Course Contents

Unit I

Introduction to AI & Agents: Why study AI?, What is AI?, The Turing Test, Rationality, Branches and Brief History of AI, Challenges for the Future, Intelligent Agents: Definition, Rational Agents, Rationality, Performance Measure, PEAS, Agent Types: Reflex, Model-based, Goal-based, Utility-based**.**

- Pedagogy: Chalk and board, Problem based learning, Visual Aids
- Link: https://nptel.ac.in/courses/106106126

Unit II

Search & Problem Solving: Problem-solving agents, problem formulation, Grid world and Vacuum world, Uninformed Search: DFS, BFS, DLS, IDS, Informed Search: Best-First, A*, Heuristic Search

- Pedagogy: Chalk and board, Problem based learning, Pair Programming
- Link: https://nptel.ac.in/courses/106106126

Unit III

Problem Reduction & Reasoning: Problem Reduction: AO* Algorithm, Game Playing: Minimax, Alpha-Beta Pruning, Introduction to Knowledge-Based Agents, Wumpus World, FOL

- Pedagogy: Chalk and board, Problem based learning, Role Play
- Link: https://nptel.ac.in/courses/106106126

Unit IV

Fundamentals of Machine Learning: Supervised vs. Unsupervised Learning, Evaluation Metrics, Hypothesis Space, Inductive Bias, Linear Regression, Decision Trees, Overfitting, KNN, Cross-validation

- Pedagogy: Chalk and board, Problem based learning, Case Studies
- Link : https://nptel.ac.in/courses/106106202

Unit V

Advanced ML Techniques: Logistic Regression, SVM, Kernel SVM, Neural Network: Perceptron, MLP, Backpropagation, Introduction to DNN, Clustering: K-Means, Hierarchical Clustering

- Pedagogy: Chalk and board, Problem based learning, Case Studies
- Link: https://nptel.ac.in/courses/106106213

Text Books:

1. Artificial Intelligence-A Modern Approach, Stuart J. Russell and Peter Norvig, Pearson 4th Edition, Eleventh Impression 2022.
2. Tom Mitchell, Machine Learning, First Edition, McGraw- Hill, 1997

Reference Books:

1. Ethem Alpaydin, Introduction to Machine Learning, 2nd Edition, MIT Press.2010.
2. Elaine Rich, Kevin Knight, Shivashanka B Nair: Artificial Intelligence, Tata MCGraw Hill 3rd edition. 2013
3. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow, 2nd Edition, Aurelien Geron, O'Reilly

Course Outcomes (COs):

At the end of the course student will be able to:

1. Understand foundational concepts, history, and scope of Artificial Intelligence. (PO-1,2,3 PSO-1)
2. Analyze AI solutions using search and agent models. (PO-1,2,3,4,5 PSO-1,2)
3. Demonstrate logical reasoning and game-playing using suitable algorithms. (PO-1,2,3,4,5 PSO-1,2)
4. Apply machine learning algorithms to classification and prediction tasks. (PO- 1,2,4,5 PSO-1,2)
5. Evaluate advanced models using neural networks and clustering techniques. (PO-1,2,3,4,5 PSO-1,2)

Course Assessment and Evaluation:

Continuous Internal Evaluation (CIE): 50 Marks		
Assessment Tools	**Marks**	**Course Outcomes addressed**
Internal Test-I (CIE-I)	30	CO1, CO2
Internal Test-II CIE-II)	30	CO3, CO4, CO5
The average of the two CIE shall be taken for 30 marks		
Other Components		
Tutorial Assignment-1	10	CO1, CO2, CO3
Tutorial Assignment-2	10	CO3, CO4, CO5
The Final CIE out of 50 Marks = Average of two CIE tests for 30		
Semester End Examination (SEE)	100	CO1, CO2, CO3, CO4, CO5

ADVANCED COMPUTER NETWORKS	
Course Code: CY52	**Credits: 2:0:1**
Prerequisite: Nil	**Contact Hours: 28L+14P**
Course Coordinator: Dr. Josy Elsa Varghese	

Course Contents

Unit I

Network layer: Logical addressing - IPV4 addresses, Address space, notations, classful and classless addressing with problem solving, NAT, IPV6 addresses; IPV6 addresses; **Network layer: Internet protocol** - IPV4 datagram, fragmentation, checksum and options; IPV6 packet format, advantages and extension headers; Transition from IPV4 to IPV6.

- Pedagogy: Chalk and Talk, PowerPoint Presentations
- Link: https://onlinecourses.nptel.ac.in/noc22_cs19/

Unit II

Address mapping, Error reporting, & Multicasting - Address mapping, ARP, RARP, BOOTP and DHCP; ICMP, IGMP, **Network layer: Delivery, Forwarding, & Routing** – Direct Vs Indirect delivery, Forwarding Techniques, Forwarding Process, Routing Table, **Unicast routing protocols with problem solving** – Optimization, Intra and Inter domain routing, distance vector routing, link state routing.

- Pedagogy: Chalk and Talk, PowerPoint Presentations
- Link: https://onlinecourses.nptel.ac.in/noc22_cs19/

Unit III

Multicast routing protocols – Introduction, applications, unicast routing vs multicast routing, source-based tree routing, group shared tree routing. **Transport Layer** - Process-to-Process delivery, User Datagram Protocol, Transmission Control Protocol.

- Pedagogy: Chalk and Talk, PowerPoint Presentations
- Link: https://onlinecourses.nptel.ac.in/noc22_cs19/

Unit IV

Congestion control & QOS - Data traffic, Congestion, Congestion control, Two examples – congestion control in TCP and Frame Relay, Quality of Service, Techniques to improve QOS.
Application Layer: Domain Name System - Namespace, Domain name space, Distribution of Name space, DNS in internet, Resolution.

- Pedagogy: Chalk and Talk, PowerPoint Presentations
- Link: https://onlinecourses.nptel.ac.in/noc22_cs19/

Unit V

Remote logging – TELNET; Electronic mail – Architecture, User Agent, Message Transfer Agent: SMTP; File transfer - File transfer protocol (FTP),

Network Management: SNMP - Network management system, Simple Network Management Protocol – concept, management components (Basic overview).

- Pedagogy: Chalk and Talk, PowerPoint Presentations
- Link: https://onlinecourses.nptel.ac.in/noc22_cs19/

Text Books:

1. Behrouz A. Forouzan, Data Communications and Networking, Fourth Edition, Tata McGraw-Hill, 2006.

References:

1. Behrouz A. Forouzan, Data Communications and Networking with TCPIP Protocol Suite| 6th Edition, McGraw-Hill, 2022.
2. Wayne Tom,asi, Introduction to Data Communications and Networking, Pearson Education, 2005.
3. Alberto Leon-Garcia and Indra Widjaja, Communication Networks –Fundamental Concepts and Key architectures, Second Edition, Tata McGraw-Hill, 2004.

Course Outcomes (COs):

At the end of the course, students will be able to

1. Understand IPv4 and IPv6 addressing schemes, network layer protocols, and the transition from IPv4 to IPv6.(PO-1, 2, 3,5) (PSO-1, 2)
2. Describe address mapping techniques , error reporting protocols ,packet delivery, forwarding, and routing algorithms.(PO-1, 2, 3,5) (PSO-1, 2)
3. Analyze multicast routing protocols, key transport layer protocols for process-to-process communication.(PO-1, 2, 3,5) (PSO-1, 2)
4. Analyze different techniques to improve transport layer protocols and QOS (PO-1, 2, 3,5) (PSO-1,2)
5. Demonstrate the working of various application layer protocols and network management . (PO-1,2, 3,5) (PSO-1,2)

Course Assessment and Evaluation:

Continuous Internal Evaluation: 50 Marks		
Assessment Tool	**Marks**	**Course outcomes addressed**
Internal test-I	30	CO1, CO2, CO3
Internal test-II	30	CO3, CO4, CO5
Average of the two internal tests shall be taken for 30 marks.		
Other components		
Assignment 1	10	CO1, CO2, CO3
Assignment 2	10	CO1, CO2, CO3, CO4, CO5
Semester End Examination (SEE)	100	CO1, CO2, CO3, CO4, CO5

CRYPTOGRAPHY AND NETWORK SECURITY	
Course Code: CY53	**Credits: 4:0:0**
Prerequisite: Nil	**Contact Hours: 56L**
Course Coordinator: Mrs. Shankaramma	

Course Contents

Unit I

Overview: Computer Security Concepts, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, A Model for Network Security. **Classical Encryption Techniques**: Symmetric Cipher Model: Cryptography, Cryptanalysis and BruteForce Attack, Substitution Techniques: Caesar Cipher, Mono-alphabetic Cipher, Playfair Cipher, Poly alphabetic Cipher..

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Unit II

Block Ciphers and the data encryption standard: Stream Ciphers and Block Ciphers, the Feistel Cipher, DES encryption, DES decryption. A DES example: Results, The Avalanche effect, The Strength of DES: The Use of 56-Bit Keys, the nature of the DES algorithm, timing attacks, Block Cipher Design Principles: Number of rounds, Design of function F, Key schedule Algorithm. **Advanced Encryption Standard**: AES structure, AES Transformation Functions, AES Key Expansion.

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Unit III

Public-Key Cryptography and RSA: Principles of public-key cryptosystems: Public-key cryptosystems. Applications for public-key cryptosystems, Requirements for public-key cryptosystems. Public-key cryptanalysis. **The RSA algorithm**: Description of the algorithm, computational aspects, the security of RSA. **Other Public Key Cryptosystems**: Diffie Hellman Exchange: The Algorithm, Key Exchange Protocols, Man in the middle attack.

- Pedagogy: Chalk and Talk, PowerPoint Presentations, Active Learning

Unit IV

Key Management and Distribution: Distribution of Public Keys: Public Announcements of Public Keys, Public Available Directory, Public Key Authority, Public Key Certificates, X-509 certificates. Certificates, X-509 version 3, Kerberos, Kerberos version 4. **Web Security Considerations**: Web Security Threats, Web Traffic Security Approaches.

- Pedagogy: Chalk and Talk, PowerPoint Presentations.

Unit V

Secure Sockets Layer: SSL Architecture, SSL Record Protocol, Change Cipher Spec Protocol, Alert Protocol, and Handshake Protocol, Cryptographic Computations. **Transport Layer Security**: Version Number, Message Authentication Code, Pseudorandom Functions, Alert Codes, Cipher Suites, Client Certificate Types, Certificate Verify and Finished Messages, Cryptographic Computations, and Padding. HTTPS Connection Initiation, Connection Closure. Secure Shell(SSH) Transport Layer Protocol, User Authentication Protocol, Connection Protocol. **Electronic Mail**

Security: Pretty Good privacy, S/MIME.

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Text Books:

1. William Stallings, "Cryptography and Network Security", Pearson Education, 6th ed, 2013.

References:

1. William Stallings, "Network Security Essentials Applications and Standards", 2nd ed., Pearson Education, 2003.
2. Charlie Kaufman, Radis Perlman and Mike Speciner, "Network Security – Private Communication in a Public World" 2nd ed., Pearson Education, 2003.
3. Cyrus Piekari, Anton Chuvakin, "Security Warrior", 2nd ed., Oreilly Publishers, 2005.
4. Peborab Russell, G.T. Gangeni Sr, "Computer Security Basics", 2 nd ed., O'reilly Publishers, 2006.

Course Outcomes (COs):

At the end of the course the student will be able to:

1. Describe computer security concepts,security attacks, services, mechanisms, and the OSI security architecture. (PO 1,2 ,PSO-1)
2. Apply classical encryption techniques, symmetric encryption algorithms such as DES and AES. (PO 1,2,3,5 , PSO-1,2,3)
3. Implement public-key cryptography algorithms like RSA and Diffie-Hellman, and analyse their security. (PO 1,2,3,4,5, PSO-1,2,3)
4. Demonstrate key management techniques and user authentication protocols,Kerberos and digital certificates. (PO 1,2,3, 5 PSO-1,2,3)
5. Apply security protocols such as SSL/TLS, SSH, PGP, and S/MIME for securing web applications. (PO 1,2,3,5 ,PSO-1,2)

Course Assessment and Evaluation:

Continuous Internal Evaluation (CIE): 50 Marks		
Assessment Tools	**Marks**	**Course Outcomes (COs) addressed**
Internal Test-I (CIE-I)	30	CO1, CO2
Internal Test-II CIE-II)	30	CO3, CO4, CO5
Average of the two CIE shall be taken for 30 marks		
Other Components		
Assignment-1	10	CO1, CO2, CO3
Assignment-2	10	CO4, CO5
The Final CIE out of 50 Marks = Average of two CIE tests for 30 Marks+ Marks scored in Assignment-1 +Marks scored in Assignment-2		
Semester End Examination (SEE)	50	CO1, CO2, CO3 CO4, CO5

SOFTWARE ENGINEERING	
Course Code: CY54	**Credits: 3:0:0**
Prerequisite: Nil	**Contact Hours: 42L**
Course Coordinator: Ms. Pallavi T P	

Course Contents

Unit I

Introduction: Professional software development, Software engineering ethics, Case studies. **Software processes:** Software process models, Process activities, coping with change, Process improvement. **Agile Software Development:** Agile methods, Agile development techniques, Agile project management, Scaling agile methods

- Pedagogy / Course delivery tools: Chalk and talk, Power point presentation, Videos
- Link: https://www.coursera.org/learn/software-processes-and-agile-practices

Unit II

Requirements Engineering: Functional and Non-functional requirements, the software requirements document, Requirements specification, Requirements Engineering Processes, Requirements elicitation and analysis, Requirements validation, Requirements management.

- Pedagogy /Course delivery tools: Chalk and talk, Power point presentation, Videos
- Link: https://www.coursera.org/specializations/requirements-engineering-secure-software https://www.coursera.org/learn/software-engineering-modeling-software-systems-using-uml

Unit III

Architectural Design: Software Design and Implementation, Architectural design decisions, Architectural views, Architectural patterns, Application architectures. **Design and Implementation:** Object-oriented design using the UML, Design patterns, Implementation issues, Open source development.

- Pedagogy / Course delivery tools: Chalk and talk, Power point presentation, Videos
- Link: https://archive.nptel.ac.in/courses/106/101/106101061/ https://archive.nptel.ac.in/courses/106/105/106105182

Unit IV

Software Testing: Development testing, Test-driven development, Release testing, User testing. **Software Evolution:** Evolution processes, Software maintenance, Legacy system management.

- Pedagogy / Course delivery tools: Chalk and talk, Power point presentation, Videos
- Link: https://archive.nptel.ac.in/courses/106/101/106101061/ https://archive.nptel.ac.in/courses/106/105/106105182/

Unit V

Project management: Risk management, Managing people, Teamwork. **Project planning**: Software pricing, Plan-driven development, Project scheduling, agile planning, Estimation techniques.

Quality management: Quality management, Software quality, Software standards, Reviews And inspections, Software measurement.

- Pedagogy / Course delivery tools: Chalk and talk, Power point presentation, Videos
- Link: https://archive.nptel.ac.in/courses/106/101/106101061/ https://www.coursera.org/learn/software-engineering-software-design-and-project- management

Textbooks:

1. Ian Sommerville, Software Engineering, 10th Edition, Pearson Education, July,2021

References:

1. Pressman, Roger S. Software Engineering: A Practitioner's Approach, 2020, 9th Edition, McGraw-Hill. ISBN 978-1-260-54800-6
2. Krief, Mikael. Learning DevOps, 2019, 1st Edition, 2019, Packt Publishing Ltd. ISBN 9781838642730

Course Outcomes (COs):

At the end of the course the student will be able to:

1. Understand the fundamentals of software development, software engineering ethics,software process models and application in project management.(PO-1,2,3,7,8,9,10, 11, PSO-1,3)
2. Analyze and document software requirements by distinguishing between functional and non-functional requirements, performing requirements elicitation, validation, and managing requirement changes effectively.(PO-1,2,3,7,8,9,10, 11, ,PSO-1,3)
3. Design software architectures and systems using architectural views, patterns, and object-oriented design principles.(PO-1,2,3,7,8,9,10, 11,12 ,PSO-1,3)
4. Understand Software testing and evolution processes. (PO-1,2,3,7,8,9,10, 11, PSO-1,3)
5. Demonstrate project management skills , risk management, team management, project planning and scheduling to ensure software standards and measurement. (PO-1,2,3,7,8,9,10,11,12 , PSO-1,3)

Course Assessment and Evaluation:

Continuous Internal Evaluation (CIE): 50 Marks		
Assessment Tool	**Marks**	**Course outcomes addressed**
Internal test-I	30	CO1, CO2, CO3
Internal test-II	30	CO3, CO4, CO5
The average of two internal tests shall be taken for 30 marks.		
Other components		
Assignment 1- Certification courses	10	CO1, CO2, CO3,CO4,CO5
Assignment 2- Project Development	10	CO1, CO2, CO3, CO4, CO5
Semester End Examination (SEE)	100	CO1, CO2, CO3, CO4, CO5

Secure Coding using C/C++

Course Code: CYE551	**Credits: 3:0:0**
Prerequisite: Nil	**Contact Hours: 42L**
Course Coordinator: Mrs. Shankaramma	

Course Contents

Unit I

Running with Scissors: Gauging the Threat, Security Concepts, Development Platforms, **Strings**: Character Strings, Common String Manipulation Errors, String Vulnerabilities and Exploits, Mitigation Strategies for Strings, String- Handling Functions.

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Unit II

Pointer Subterfuge: Data Locations, Function Pointers, Object Pointers, Modifying the Instruction Pointer, Global Offset Table, The .dtors Section, Virtual Pointers, The atexit() and on_exit() Functions, The longjmp() Function, Exception Handling. **Dynamic Memory Management**: C Memory Management, Common C Memory Management Errors, C++ Dynamic Memory Management, Common C++ Memory Management Errors.

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Unit III

Memory Managers, Doug Lea's Memory Allocator, Buffer Overflows on the Heap, Notable Vulnerabilities. **Integer Security**: Introduction to Integer Security, Integer Data Types, Integer Conversions, Integer Operations.

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Unit IV

Integer Vulnerabilities, Mitigation Strategies. **Formatted Output**: Variadic Functions, Formatted Output Functions, Exploiting Formatted Output Functions, Stack Randomization, Notable Vulnerabilities.

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Unit V

File I/O: File I/O Basics, File I/O Interfaces, Access Control, File Identification, Race Conditions, **Recommended Practices**: The Security Development Lifecycle, Security Training.

- Pedagogy: Chalk and Talk, PowerPoint Presentation

Text Books:

1. Robert C. Seacord: Secure Coding in C and C++, 2nd Edition, Pearson, 2013. (Chapter 1,2,3,4,5,6,8,9).

References:

1. SEI CERT Coding Standard

Course Outcomes (COs):

At the end of the course, students will be able to

1. Understand the vulnerability associated with Sting Handling and Mitigation strategies. (PO1,2,3,PSO-1,2)
2. Describe the threats associated with Runtime Memory Management and Pointers. (PO1,2,3,PSO-1,2)
3. Apply the mitigation techniques for vulnerable memory management and data type conversion. (PO1,2,3,4,5,PSO-1,2)
4. Identify the vulnerability associated with Formatted Output and Concurrency (PO1,2,3,PSO-1,2)
5. Describe the vulnerability mitigation techniques for File I/O and recommended practices for security development lifecycle. (PO1,2,3,8,PSO-1,2,3)

Course Assessment and Evaluation:

Continuous Internal Evaluation (CIE): 50 Marks		
Assessment Tools	**Marks**	**Course Outcomes (COs) addressed**
Internal Test-I (CIE-I)	30	CO1, CO2
Internal Test-II CIE-II)	30	CO3, CO4, CO5
Average of the two CIE shall be taken for 30 marks		
Other Components		
Case study	10	CO1, CO2, CO3,CO4, CO5
Programming Assignment	10	CO1, CO2, CO3,CO4, CO5
The Final CIE out of 50 Marks = Average of two CIE tests for 30 Marks+ Marks scored in Case Study +Marks scored in Assignment		
Semester End Examination (SEE)	50	CO1, CO2, CO3 CO4, CO5

CYBER WARFARE	
Course Code: CYE552	**Credits: 3:0:0**
Prerequisite: Nil	**Contact Hours: 42L**
Course Coordinator: Mrs. Shankaramma	

Course Contents

Unit I

What is Cyber Warfare: What is Cyber Warfare, Have you seen a Cyber War? Why Cyber Warfare is important. **Cyber Space Battlefield**: Boundaries in Cyber Warfare, Where Cyber fits war fighting Domains, Threatscape. **Cyber Warriors**: What does a warrior looks like?.

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Unit II

Logical Weapons: Reconnaissance Tools, Scanning Tools, Access and Escalation Tools, Exfiltration Tools, Sustainable Tools, Assault Tools, Obfuscation Tools. **Physical Weapons**: How the logical and physical realms are connected, Infrastructure Concerns, Tools for physical attack and defense.

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Unit III

Psychological Weapons: Social Engineering Explained, How Military Approaches and Defends Social Engineering. **Computer Network Exploitation**: Intelligence and Counter Intelligence, Reconnaissance, Surveillance**, Computer Network Attack**: The attack process.

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Unit IV

Computer Network Defense: What We Protect, Security Awareness and Training, Defending against Cyber Attacks. **Non-State Actors in Computer Network Operations**: Individual Actors, Corporations, Cyber Terrorism, Organized Cyber Crime, Autonomous actors.

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Unit V

Legal System Impacts: Legal Systems, Key U S Laws, Privacy Impacts. **Ethics:** Ethics in Cyber Warfare **Cyberspace Challenges**: Cyber Security Issues defined. Future of Cyber warfare.

- Pedagogy: Chalk and Talk, PowerPoint Presentation.

Text Books:

1. Andress, Steve Winterfeld, Cyber Warfare: Techniques, Tacticts Tools for Security Practitioners, Elsevier, 2011

References:

1. Jeffrey Carr, “Inside Cyber Warfare: Mapping the Cyber Underworld”, O’Reilly Media 2011 1449310044.

2. Chapple Mark and David Seidl, “Cyberwarfare: Information Operations in a Connected World - with Cloud Labs”, 2 Editions. Burlington, MA: Jones & Bartlett, 2022, ISBN-13: 978-1-284-53723-9.

Course Outcomes (COs):

At the end of the course, students will be able to

1. Understand the importance of information, targets and combatants of cyberwarfare (PO 1,2,3,PSO-1,2)
2. Illustrate the role of law and ethics in cyberwarfare, intelligence operations in cyberwarfare (PO 1,2,3, 6,8,PSO-1,2,3).
3. Analyze the cyberwarfare attackers and the evolution of cyberwarfare techniques. (PO 1,2,3, 6,8,PSO-1,2,3)
4. Describe the significance of cryptography in cyberwar and defense-in-depth strategies. (PO 1,2, 3,PSO-1,2).
5. Discuss the legal System Impact and cyber space challenges(PO 1,2,3, 6,8,PSO-1,2,3).

Course Assessment and Evaluation:

Continuous Internal Evaluation (CIE): 50 Marks		
Assessment Tools	**Marks**	**Course Outcomes (COs) addressed**
Internal Test-I (CIE-I)	30	CO1, CO2
Internal Test-II CIE-II)	30	CO3, CO4, CO5
Average of the two CIE shall be taken for 30 marks		
Other Components		
Case study	10	CO1, CO2, CO3
Assignment	10	CO4, CO5
The Final CIE out of 50 Marks = Average of two CIE tests for 30 Marks+ Marks scored in Case Study +Marks scored in Assignment		
Semester End Examination (SEE)	50	CO1, CO2, CO3 CO4, CO5

IDENTITY ACCESS MANAGEMENT	
Course Code: CYE553	**Credits: 3:0:0**
Prerequisite: Nil	**Contact Hours: 42L**
Course Coordinator: Ms. Kavya Natikar	

Course Contents

Unit I

Identification, Authentication, Authorization & Accounting (IAAA): Introduction, CIA Principles, IAAA operation, Kerberos,Web Services Federation and OAuth, Some Important Security Concepts, Identity federation & SSO, Authentication Factors, Biometrics.

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Unit II

Identity Governance and Administration (IGA) : Domain 3 Identity Governance and Administration (IGA), User Onboarding,User Termination & Role changes, Access Controls & RBAC, Access validation & Certification, Segregation of Duties, Auditing and Reporting, Identity Lifecycle Management (ILM), System for Cross-domain Identity Management.

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Unit III

Access Control and identity life cycle management: Control Physical and Logical Access, Types of Access Controls, Groups and Roles, Session Management, Registration and Proofing, FIM, Credential Management, SSO and Just-in-Time.

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Unit IV

Key Identity and Access Management Concepts: Identification Proofing, The Fundamental Process of Identification, Authentication Reuse, RFID Tokens, Biometric Consideration, Authorization, Data Visibility, Access Control Models, Comparing Access Control Models, Privileged Access Management.

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Unit V

Technologies in Identity Access Management: Forms of Authentication Kerberos, Technologies Relating to Identity and Access Management, Open Authorization, Secure Sockets Layer and Transport Layer Security, Open System Interconnected Model, Public Key Infrastructure, Active Directory and LDAP.

- Pedagogy: Chalk and Talk, PowerPoint Presentations.

Reference links:

1. https://alison.com/course/identity-and-access-management
2. https://www.udemy.com/course/identity-and-access-management-iam/?couponCode=MT300725A
3. https://www.coursera.org/learn/packt-identify-andaccess-management-iam-oy5r6#modules.

Course Outcomes (COs):

At the end of the course the student will be able to:

1. Understand the importance of Identity IAAA (Identification, Authentication, Authorization, Accounting) (PO-1, PSO-2)
2. Analyse Identity Governance and Administration (IGA) (PO-1,2,3 PSO-2)
3. Understand Access Control and identity life cycle management (PO-1,2,3 PSO-2)
4. Analyse Key Identity and Access Management Concepts (PO-1, PSO-2)
5. Apply Technologies in Identity Access Management (PO-1,2,3,4 PSO-2)

Course Assessment and Evaluation:

Continuous Internal Evaluation (CIE): 50 Marks		
Assessment Tools	**Marks**	**Course Outcomes (COs) addressed**
Internal Test-I (CIE-I)	30	CO1, CO2
Internal Test-II CIE-II)	30	CO3, CO4, CO5
Average of the two CIE shall be taken for 30 marks		
Other Components		
Assignment 1	10	CO1, CO2, CO3
Assignment 2	10	CO4, CO5
The Final CIE out of 50 Marks = Average of two CIE tests for 30 Marks+ Marks scored in Case Study +Marks scored in Assignment		
Semester End Examination (SEE)	50	CO1, CO2, CO3 CO4, CO5

BLOCKCHAIN TECHNOLOGY

Course Code: CYE554	**Credits: 3:0:0**
Prerequisite: Nil	**Contact Hours: 42L**
Course Coordinator: Dr. Anjaneyulu Pasala/ Chethan Sharma	

Course Contents

Unit I

Basics of Blockchain: Introduction, Concept of Blockchain, Definition of Blockchain, Fundamentals of Blockchain, Characteristics of Blockchain, Consensus in Trust-Building Exercise, Public, Private, and Hybrid Blockchains, Distributed Ledger Technologies, Architecture of Blockchain Transactions, Chaining Blocks, **Decentralized System:** Distributed Decentralized Databases Decentralized Enterprise, Decentralization, Disintermediation.

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Unit II

Hash Functions: Introduction, Hashing, Message Authentication Code, Secure Hash Algorithms (SHA-1), Secure Hash Algorithm Version 3, Distributed Hash Tables, Hashing and Data Structures, hashing in Blockchain Mining.

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Unit III

Blockchain Components: Introduction, Ethereum, Ethereum Virtual Machine, Working of Ethereum, Ethereum Clients, Ethereum Key Pairs, Ethereum Addresses, Ethereum Wallets, Ethereum Transactions, Ethereum Languages.

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Unit IV

Smart Contracts: Introduction, Absolute and Immutable, Contractual Confidentiality, Law Implementation and Settlement, Characteristics, Internet of Things, Utilities: Smart Grid, Proofs of Origin, Supply Chain Management, Medical Sciences, Finance, Media and Entertainment, Public Services, Legal Services, Darknet.

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Unit V

Bitcoins: Introduction, Working of Bitcoin, Merkle Trees, Bitcoin Block Structure. **Decentralized Applications**: Introduction, Today's Web Applications Requirement, Mining in Blockchain Bitcoin, Blocks Validation and Identification.

Blockchain Vertical Solutions and Use Cases: Blockchain, Blockchain in Insurance, Life Insurance and Claim Processing in Case of Death, Healthcare, Assets Management, Financial Institutional Assets, Smart Assets.

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Text Book:

1. Blockchain Technology: Concepts and Applications, Kumar Saurabh, Ashutosh Saxena , Wiley, ISBN: 9788126557660

Reference Book:

1. Blockchain Applications: A Hands-On Approach, Arshdeep Bahga, Vijay Madisetti, 1st Edition, VPT, 2017.
2. Mastering Bitcoin: Programming the Open Blockchain, Andreas M. Antonopoulos, 2nd Edition, O'Reilly Media, 2017.
3. Mastering Blockchain, Imran Bashir, 2nd Edition, Packt Publishing, 2018

Course Outcomes (COs):

At the end of the course, students should be able to:

1. Understand the fundamentals, architecture, types of blockchain and decentralized systems.(PO1,2,3,PSO-1,2)
2. Analyze hash functions and consensus algorithms used in blockchain technology.(PO1,2,3,PSO-1,2)
3. Understand the components and operations of Ethereum and its ecosystem.(PO1,2,3,PSO-1,2)
4. Apply blockchain concepts to real-world applications.(PO1,2,3,5,PSO-1,2)
5. Analyze Bitcoin structure, decentralized applications, and blockchain use cases(PO1,2,3,PSO-1,2)

Course Assessment and Evaluation:

Continuous Internal Evaluation (CIE): 50 Marks		
Assessment Tool	**Marks**	**Course outcomes addressed**
Internal test-I	30	CO1, CO2, CO3
Internal test-II	30	CO3, CO4, CO5
Average of the two internal tests shall be taken for 30 marks.		
Other components		
Seminar	10	CO1, CO2, CO3
Assignment	10	CO3, CO4, CO5
Semester End Examination (SEE)	100	CO1, CO2, CO3, CO4, CO5

INTERNET OF THINGS	
Course Code: CYE555	**Credits: 3:0:0**
Prerequisite: Nil	**Contact Hours: 42L**
Course Coordinator: Dr. Mohan Kumar S	

Course Contents

Unit I

What is IoT, Genesis of IoT, IoT and Digitization, IoT Impact, Convergence of IT and IoT, IoT Challenges, IoT Network Architecture and Design, Drivers Behind New Network Architectures, Comparing IoT Architectures, A Simplified IoT Architecture, The Core IoT Functional Stack, IoT Data Management and Compute Stack.

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Unit II

Smart Objects: The "Things" in IoT, Sensors, Actuators, and Smart Objects, Sensor Networks, Connecting Smart Objects, Communications Criteria, IoT Access Technologies.

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Unit III

IP as the IoT Network Layer, The Business Case for IP, The need for Optimization, Optimizing IP for IoT, Profiles and Compliances, Application Protocols for IoT, The Transport Layer, IoT Application Transport Methods

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Unit IV

Data and Analytics for IoT, An Introduction to Data Analytics for IoT, Machine Learning, Big Data Analytics Tools and Technology, Edge Streaming Analytics, Network Analytics, Securing IoT, A Brief History of OT Security, Common Challenges in OT Security, IoT Physical Devices and Endpoints - Arduino UNO: Introduction to Arduino, Arduino UNO, Installing the Software, Fundamentals of Arduino Programming.

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Unit V

IoT Physical Devices and Endpoints - RaspberryPi: Introduction to RaspberryPi, About the RaspberryPi Board: Hardware Layout, Operating Systems on RaspberryPi, Configuring RaspberryPi, Programming RaspberryPi with Python, Wireless Temperature Monitoring System Using Pi, DS18B20 Temperature Sensor, Connecting Raspberry Pi via SSH, Accessing Temperature from DS18B20 sensors, Remote access to RaspberryPi, Smart and Connected Cities, An IoT Strategy for Smarter Cities, Smart City IoT Architecture, Smart City Security Architecture, Smart City Use-Case Examples.

- Pedagogy: Chalk and Talk, PowerPoint Presentation

Textbooks:

1. David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, Jerome Henry,"IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things", 1st Edition, Pearson Education (Cisco Press Indian Reprint). (ISBN: 978- 9386873743)

Reference Books:

1. Raj Kamal, "Internet of Things: Architecture and Design Principles", 1st Edition, McGraw Hill Education, 2017. (ISBN: 978-9352605224)

Course Outcomes (COs):

At the end of the course, students should be able to:

1. Grasping the core concepts, architecture, and enabling technologies of IoT (PO: 1,2,5 PSO: 2,3)
2. Design in programming microcontrollers (like Arduino) and microprocessors (like Raspberry Pi) for IoT devices (PO: 1,2,5 PSO: 2, 3)
3. Ability to interface sensors and actuators with embedded systems to collect and interact with the physical world. (PO: 1,2,5 PSO: 2, 3)

Course Assessment and Evaluation:

Continuous Internal Evaluation: 50 Marks		
Assessment Tool	**Marks**	**Course outcomes addressed**
Internal test-I	30	CO1, CO2
Internal test-II	30	CO2, CO3
Average of the two internal tests shall be taken for 30 marks.		
Other components		
Assignment 1	10	CO1, CO2, CO3
Assignment 2	10	CO1, CO2, CO3
Semester End Examination (SEE)	100	CO1, CO2, CO3

APPLICATION DEVELOPMENT USING JAVA LABORATORY

Course Code: CYL56	**Credits: 0:0:1**
Prerequisite:	**Contact Hours: 14P**
Course Coordinator: Mrs. Akshatha G C	

Course Contents

1. Introduction to Java: Overview of Java Data types, Variables, arrays, Control statements.
2. OOPs Concepts: Classes, Objects, Methods and Constructors.
3. Code reusability using Inheritance and Abstract classes.
4. Multi-threaded applications, Packages and interfaces.
5. Exception handling, collections framework.
6. Database connectivity using JDBC.
7. Web-based app development using Servlets, JSP, XML, 3-tier architecture.
8. Remote Method Invocation.

Text Books:

1. Herbert Schildt, Java: The Complete Reference, Eleventh Edition, 2019.

Course Outcomes (COs):

At the end of the course students will be able to:

1. Develop real time applications using Object oriented features in Java. (PO-1,2,3,4,5, 8, 9,10,12, PSO-1,2 3)
2. Demonstrate database connectivity using JDBC. (PO-1,2,3,4,5, 8, 9,10,12, PSO-1,2)
3. Develop web applications using servlets, JSP and RMI. (PO-1,2,3,4,5, 8, 9,10,12, PSO-1,2)

Course Assessment and Evaluation:

Parameter	**Marks**
CIE Test	20
Lab Record Writing + Viva+ Weekly Evaluation	30
Total	**50**
Final Exam will be conducted for 50 marks (SEE)	

CRYPTOGRAPHY AND NETWORK SECURITY LAB	
Course Code: CYL57	**Credits: 0:0:1**
Prerequisite: Nil	**Contact Hours: 14P**
Course Coordinator: Mrs. Shankaramma	

Course Contents

Part A

1. Develop a Java program to implement Caesar Cipher, Perform encryption and decryption with a user-defined shift value.
2. Develop a Java program to implement Playfair Cipher, encrypt a given plaintext using 5x5 matrix.
3. Develop a Java program to implement DES Algorithm. Simulate DES encryption and decryption using Java's security libraries or custom logic.
4. Write a Java program to implement AES Algorithm, use Java Cryptography Extension (JCE) to perform AES encryption and decryption with a 128-bit key.
5. Write a Java program to implement RSA Algorithm, generate public/private key pairs, encrypt a message with the public key, and decrypt using the private key.

Part B

1. Use Wireshark to capture and analyse SSL/TLS handshake. Perform a secure browser transaction and analyze packet-level handshake.
2. Capture and analyse HTTP/2 traffic over TLS using Wireshark. Open a modern website that supports HTTP/2 and inspect the protocol negotiation, multiplexed streams, and TLS encryption.
3. Initiate an SSH session between two local systems or virtual machines. Capture traffic using Wireshark and analyse the session key exchange, encryption setup, and user authentication.
4. Use a packet crafting tool such as Scapy (Python) to create custom TCP, UDP, or ICMP packets. Send these packets to a target system and observe how a firewall responds. Use Wireshark to capture and analyze the traffic, including flags, headers, and dropped packets.
5. Simulate an ARP spoofing attack in a controlled local network using tools like arpspoof or Ettercap. Capture the ARP traffic with Wireshark to observe the malicious ARP replies and analyze how the attacker intercepts traffic (Man-in-the-Middle).

Text Book:

1. "Cryptography and Network Security: Principles and Practice" by William Stallings, 7th Edition URL: https://williamstallings.com/Crypto/Crypto7e.html

Reference Book:

1. "Network Security Essentials: Applications and Standards" by William Stallings, 6th Edition, 2013

Course Outcomes (COs):
At the end of the course, the students should be able to:

1. Implement encryption and decryption algorithms to protect the network resources. (PO 1,2,3,4,5,10, PSO 1,2,3)
2. Apply key management and digital identity for digital signatures and demonstrate their utility in securing digital communication.(PO 1,2,3,4,5,10, PSO 1,2,3)
3. Demonstrate network security concepts to ensure secure transmission of information across communication networks(PO 1,2,3,4,5,10, PSO 1,2,3)

Course Assessment and Evaluation:

Parameter	**Marks**
CIE Test	20
Lab Record Writing + Viva+ program execution	30
Total	**50**
Final Exam will be conducted for 50 marks (SEE)	

RESEARCH METHODOLOGY & INTELLECTUAL PROPERTY RIGHTS	
Course Code: AL58	**Credits: 3:0:0**
Prerequisite: Nil	**Contact Hours: 42L**
Course Coordinator: Dr. Mohana Kumar S	

Unit I

Research Methodology Introduction: Meaning of Research, Objectives of Research, Types of Research, Ethics in Research, Types of Research Misconduct. Literature Review and Technical Reading, New and Existing Knowledge, Analysis and Synthesis of Prior Art, Bibliographic Databases, Conceptualizing Research, Critical and Creative Reading.

Citations: Functions and Attributes, Impact of Title and Keywords on Citations, Knowledge flow through Citations, Acknowledgments, and Attributions.

- Pedagogy: Chalk and Talk, PowerPoint Presentations
- Links: https://onlinecourses.nptel.ac.in/noc22_ge08/preview

Unit II

Research Design: Need for Research Design, Important Concepts Related to Research Design: Dependent and Independent Variables, Extraneous Variable, Variable, Common Control, Confounded Relationship, Research Hypothesis, Experimental and Control Groups, Treatments.

Experimental Designs: Introduction to Randomised Block Design, Complete Randomised Design, Latin Square Design, and Factorial Design.

- Pedagogy: Chalk and Talk, PowerPoint Presentations
- Links: https://onlinecourses.nptel.ac.in/noc22_ge08/preview

Unit III

Method of Data Collection: Primary and Secondary Data Collection.

Sampling Design: Sampling fundamentals, Measurement, and Scaling Techniques, Criteria of Selecting a Sampling Procedure, Characteristics of a Good Sample Design, and Types of Sample Design.

Data Analysis: Testing of Hypotheses: Null Hypothesis, Alternative Hypothesis, Type I and Type II Errors, Level of Significance. Procedure for Hypothesis Testing: Mean, Variance, Proportions. Chi-square Test, Analysis of Variance (One Way ANOVA), and Covariance (ANOCOVA)

- Pedagogy: Chalk and Talk, PowerPoint Presentations
- Links: https://onlinecourses.nptel.ac.in/noc22_ge08/preview

Unit IV

Intellectual Property Rights: Introduction to IPR: Different forms of IPR, Role of IPR in Research and Development. TRIPS Agreement, Patent Cooperation Treaty (PCT).

Patents: Brief history of Patents-Indian and Global Scenario, Principles Underlying Patent Law, Types of Patent Applications in India, Procedure for Obtaining a Patent. Non-patentable Inventions. Rights Conferred to a Patentee, Basmati Rice Patent Case.

- Pedagogy: Chalk and Talk, PowerPoint Presentations
- Links: https://onlinecourses.nptel.ac.in/noc22_ge08/preview

Unit V

Design: What is a Design? Essential Requirements for a Registrable Design, Procedure of Registration of a Design.

Trademarks: Essentials of a Trademark, Registration, and Protection of Trademarks, Rights Conferred by Registration of Trademarks, Infringements, Types of Reliefs, Case Studies.

Copyrights: Characteristics of Copyrights, Rights Conferred by Registration of Copyrights, Registration of Copyrights, Infringements, Remedies against Infringement of Copyrights, Case studies

- Pedagogy: Chalk and Talk, PowerPoint Presentations
- Links: https://onlinecourses.nptel.ac.in/noc22_ge08/preview

Textbooks:

1. C. R Kothari, Gourav Garg, Research Methodology – Methods and Techniques. New Age International Publishers.
2. Dr. B L Wadehra – Law relating to Intellectual property. Universal Law Publishing Co.
3. Dipankar Deb, Rajeeb Dey, Valentina E. Balas ―Engineering Research Methodology‖, ISSN 1868-4394 ISSN 1868-4408 (electronic), Intelligent Systems Reference Library, ISBN 978-981-13-2946-3 ISBN 978-981-13-2947-0 (eBook), https://doi.org/10.1007/978-981-13-2947-0.

References:

1. David V. Thiel ―Research Methods for Engineers‖ Cambridge University Press, 978-1-107-03488-4

Course Outcomes (COs):

At the end of the course, the student will be able to:

1. Possess the knowledge of research and conduct a literature review. (PO-8, PO-10, PO-12)
2. Apply the knowledge of research design and design of experiments. (PO-4, PO-8, PO 10, PO-12)
3. Analyse data collection methods, analysis, and sampling design. (PO-4, PO-8, PO-10, PO-12)
4. Understand the global and Indian scenarios of patents and patent applications. (PO-8, PO-10, PO-12)
5. Acquire the requirements of registration and infringements related to trademarks, copyrights, and designs. (PO-8, PO-10, PO-12)

DevOps	
Course Code: CYAEC59	**Credits: 1:0:0**
Prerequisite: Nil	**Contact Hours: 14L**
Course Coordinator: Mrs. Bhavya Jyothi. A	

Course Contents:

Unit 1

Introduction: DevOps Overview and Foundations- What is DevOps, Agile Infrastructure, DevOps Culture, DevOps Engineer, DevOps Lifecycle, DevOps Pipeline, Cloud Computing, Virtualization, Cloud Providers.

Unit 2

Build Tools: Git- Git Basics, Repository, Branching / Merging, Git Workflow. **Maven, -** Maven, POM (Project Object Model, **Gradle -**Gradle, Groovy / Kotlin DSL, Build Lifecycle, Dependency Management, Build Automation.

Unit 3

Continuous Integration with Jenkins- Introduction to Jenkins, Continuous Integration (CI) with Jenkins Pipeline, Freestyle Job ,Source Code Management, Jenkins Plugins, Build Triggers, Post-build Actions, Slave Nodes

Unit 4

Configuration Management using Ansible- Why Configuration Management? Ansible Architecture & Requirements, YAML, Playbooks, Modules, Variables, Handlers, Roles and Reusability, Ansible Galaxy.

Unit 5

Kubernetes - Overview,Pods, Replica Sets, Deployments, Namespaces,Services and Networking, Persistent Volumes (PV) and Persistent Volume Claims (PVC), Labels, Selectors, Jobs, and Schedulers, Capstone: Deploy and Manage a Sample App on Kubernetes Cluster **Scaling**: Understanding Scaling, Teams & Tools in DevOps.

Textbooks:

1. Jennifer Davis and Katherine Daniels, “Effective DevOps”, 1st Edition, Shroff / O’Reilly Publications, 2021. (ISBN-13: 978-9352133765)

2. The DevOps Adoption Playbook: A Guide to Adopting DevOps in a Multi-Speed IT Enterprise 1st Edition, by Sanjeev Sharma.

Course Outcomes(CO) :

At the end of the course, the students should be able to:

1. Understand DevOps principles, culture, and cloud infrastructure (PO 1,2,3, PSO 1,2)
2. Demonstrate version control using Git, Maven, and Gradle for managing source code.(PO 1,2,3,5,9,10, PSO 1,2)
3. Implement continuous integration workflows using Jenkins, source control integration, and distributed builds.(PO 1,2,3,5,9,10, PSO 1,2)
4. Describe the infrastructure management using Ansible playbooks.(PO 1,2,3,5,9,10,PSO 1,2)
5. Explain the concepts of Kubernetes and deployment of applications. (PO 1,2,3,5,9,10,PSO 1,2)

Course Assessment and Evaluation:

Continuous Internal Evaluation (CIE): 50 Marks		
Assessment Tools	**Marks**	**Course Outcomes (COs) addressed**
Internal Test-I (CIE-I)	30	CO1, CO2
Internal Test-II CIE-II)	30	CO3, CO4, CO5
Average of the two CIE shall be taken for 30 marks		
Other Components		
Project based learning	20	20
The Final CIE out of 50 Marks = Average of two CIE tests for 30 Marks+ Marks scored in Case Study Implementation		
Semester End Examination (SEE)	50	CO1, CO2, CO3 CO4, CO5

CYBER LAW

Course Code: CYAEC59	**Credits: 1:0:0**
Prerequisite: Nil	**Contact Hours: 14L**
Course Coordinator: Dr. Mohana Kumar S	

Course Contents

Unit 1

Cyber law: Features of Cyber Law - Significance of Cyber Law - Advantages. Data Security - Meaning - Fundamentals of Data Security - Requirements of Data Security - Precautionary Measures.

Unit 2

Tools Used in Cyber crime: Proxy Servers and Anonymizers, Phishing, Password Cracking, Key loggers and Spywares, Virus and Worms, Steganography.

Unit 3

Cybercrimes and Cyber security: The Legal Perspectives Why do we need Cyber law: The Indian Context, The Indian IT Act, Digital Signature and the Indian IT Act, Amendments to the Indian IT Act, Cybercrime and Punishment, Cyber law, Technology and Students: Indian Scenario.

Unit 4

Hackers & its Types - Cracking - Pornography - Software privacy - Data Recovery - File Modification & File access, Recover Internet Usage Data, Recover Swap Files/Temporary/Cache Files, and Introduction to Encase Forensic.

Unit 5

Concept of Cyber law and Cyber Space: Introduction - Meaning and Features of Cyber law - Significance and Advantages of Cyber Law - Meaning of Cyber Space - Inclusive of Cyber Space - Facilitating Functions of Cyber Space - Major Issues in Cyber Space.

Textbooks:

1. Sunit Belapure and Nina Godbole. Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives. Wiley India Pvt Ltd. 2013.
2. Jonathan Rosenoer , Cyber law: The Law of Internet, Springer Verlog, Paperback, 17 September 2011
3. John W Ritting House, William M.Hancock, Cyber Security Operations Handbook, Read Elsevier,2004

Course Outcomes(CO) :

At the end of the course, the students should be able to:

1. Identify the cyber security needs of an organization. (PO: 1, 2, 4, 9, 11 PSO:1,2,3)
2. Detect the cybercrime and modify security architecture for an organization. (PO: 1, 2, 4, 9, 11 PSO:1,2,3)

3. Survey operational and strategic cyber security strategies and policies L4 (Through Assignment) (PO: 1, 2, 3, 9, 11 PSO:1,2,3)

Course Assessment and Evaluation:

Continuous Internal Evaluation (CIE): 50 Marks		
Assessment Tools	**Marks**	**Course Outcomes (COs) addressed**
Internal Test-I (CIE-I)	30	CO1, CO2
Internal Test-II CIE-II)	30	CO3, CO4, CO5
Average of the two CIE shall be taken for 30 marks		
Other Components		
Case study Implementation	20	20
The Final CIE out of 50 Marks = Average of two CIE tests for 30 Marks+ Marks scored in Case Study Implementation		
Semester End Examination (SEE)	50	CO1, CO2, CO3 CO4, CO5

ENVIRONMENTAL STUDIES	
Course Code: HS510	**Credits: 0:0:0 (NCMC)**
Prerequisite: Nil	**Contact Hours: 14L**
Course Coordinator: -	

Course Contents

Unit I

Environment, Ecology and Biodiversity

Definition, scope, and importance. Multidisciplinary nature of Environmental studies. Food chain and food web. Energy flow and material cycling in the ecosystem. Biodiversity and threats to biodiversity. Concept of sustainable development: Definition, objectives, and applications.

- Pedagogy/Course delivery tools: Chalk and Talk, PowerPoint presentations, Videos, Models
- Link: https://youtu.be/I_bnGkviWOU
  https://youtu.be/Ar04qG1P8Es

Unit II

Natural resources

Forest resources: Ecological importance of forests. Water resources: Global water resources distribution. Mineral resources: Environmental effects of extracting and processing Mineral resources. Food resources: Effects of modern agriculture. Land resources: Soil erosion and Desertification.

- Pedagogy/Course delivery tools: Chalk and Talk, PowerPoint presentations, Videos
- Link: https://youtu.be/vsXv3anIBSU
  https://youtu.be/1rOVPqaUy8

Unit III

Energy sources

Growing energy needs. Conventional and non-conventional / Renewable and Non-renewable energy sources. Bio Energy-Ethanol and Bio mass energy. Energy of the future – Hydrogen fuel cells and Nuclear energy. Environmental Impact Assessment (EIA): Definition, Objectives and benefits. Step by step procedure of conducting EIA.

- Pedagogy/Course delivery tools: Chalk and Talk, PowerPoint presentations, Animations, Models
- Link: https://youtu.be/mh51mAUexK4
  https://youtu.be/XS-eXqppf_w

Unit IV

Environmental pollution

Definition, Causes, Effects and control measures of Water pollution, Air pollution and Soil/ land pollution. Management of Municipal Solid Waste and treatment methods of municipal solid waste.

- Pedagogy/Course delivery tools: Chalk and Talk, PowerPoint presentations, Videos
- Link: https://youtu.be/NRoFvz8Ugeo
  https://youtu.be/DAQapF-F4Vw

Unit V

Environmental protection

Global warming and Climate change, Acid rain, Ozone layer depletion. Salient features of Environmental Protection Act, Air & Water Acts. Functions of Central and State Pollution Control Boards.

- Pedagogy/Course delivery tools: Chalk and Talk, PowerPoint presentations, Videos, Open source softwares
- Link: https://youtu.be/iV-BvYwl4Y8
  https://youtu.be/BYqLRGawo0

Text Books:

1. Dr. S M Prakash – Environmental Studies, Elite Publishers, 2007.

Reference Books:

1. P. Venugopala Rao – Principles of Environmental Science & Engineering Prentice Hall of India, 1st edition, 2006.

Web links and video Lectures (e- Resources):

1. https://youtu.be/I_bnGkviWOU
2. https://youtu.be/vsXv3anIBSU
3. https://youtu.be/mh51mAUexK4
4. https://youtu.be/NRoFvz8Ugeo
5. https://youtu.be/iV-BvYwl4Y8

Course Outcomes (COs):

At the end of the course, the student will be able to:

1. Describe the importance of environmental studies, sustainable development and biodiversity (PO-1, 7)
2. Explain the importance and conservation of impacts of natural resources (PO-1, 7)
3. Distinguish the energy sources and identify the alternative energy sources for sustainable development (PO-1, 7)
4. Identify the causes, effects and control measures of pollution in developmental activities (PO-1, 7)
5. Outline the current environmental issues and the role of the agencies for environmental protection (PO-1, 7)

Course Assessment and Evaluation:

Continuous Internal Evaluation (CIE): 50 Marks		
Assessment tool	**Marks**	**Course outcomes attained**
Internal Test-I	30	CO1, CO2, CO3
Internal Test-II	30	CO4, CO5
Average of the two internal test shall be taken for 30 marks		
Other components		
Assignment – MCQ, Objectives	10	CO1, CO2
Assignment – Quiz, Group presentation	10	CO3, CO4
Semester End Examination (SEE)	50	CO1, CO2, CO3, CO4, CO5

VI Semester

MANAGEMENT & ENTREPRENEURSHIP	
Course Code: AL61	**Credits: 3:0:0**
Prerequisite: Nil	**Contact Hours: 42L**
Course Coordinator: Dr. M Rajesh/Dr. Siddhartha Kar	

Course Contents

Unit I

Introduction to Management: Definition of Management, Its nature and purpose, Contributions of F.W. Taylor and Henry Fayol to management theory, Functions of managers.
Planning: Types of plans, Steps in planning, the planning process, Management By Objectives (MBO)
Organizing: The nature and purpose of organizing, Formal and informal organization. Organization levels and Span of management, Principle of span of management, the structure and process of organizing

- Pedagogy: Chalk board, power point presentations
- Links: https://onlinecourses.nptel.ac.in/noc23_mg33/preview
  https://www.digimat.in/nptel/courses/video/110107150/L01.html

Unit II

Staffing: Situational factors affecting staffing. Leading: Human factors in managing, definition of leadership, Ingredients of leadership
Controlling: Basic control process, Critical control points and standards, Control as a feedback system, Feed forward control, Requirements for effective controls.

- Pedagogy: Chalk board, power point presentations
- Links: https://nptel.ac.in/courses/110107150

Unit III

Introduction to Entrepreneurship: The Foundations of Entrepreneurship: What is an Entrepreneurship?, The benefits of Entrepreneurship, The potential drawbacks of Entrepreneurship; Inside the Entrepreneurial Mind: **From Ideas to Reality**: Creativity, Innovation and Entrepreneurship, Creative Thinking, Barriers to Creativity

- Pedagogy: Chalk board, power point presentations
- Links:https://www.youtube.com/watch?v=Hgj_kRrvbhQ&list=PL7oBzLzHZ1wXW3mtolxV5nIGn48NLKwrb

Unit IV

The Entrepreneurial Journey: Crafting a Business Plan: The benefits of creating a business plan, The elements of a business plan; Forms of Business Ownership and Buying an Existing Business: Sole proprietorships and partnership.

- Pedagogy: Chalk board, power point presentations
- Links:https://www.youtube.com/watch?v=Tzzfd6168jk&list=PLyqSpQzTE6M8EGZbmNUu UM7Vh2GkdbB1R

Unit V

Launching the Business: Franchising and the Entrepreneur: Types of Franchising, The benefits of buying a Franchise; E-Commerce and the Entrepreneur: Factors to consider before launching into E-commerce, Ten Myths of E-Commerce.

- Pedagogy: Chalk board, power point presentations
- Links:https://www.youtube.com/watch?v=5RMqxtMwejM&list=PLyqSpQzTE6M9zMKj_PSm81k9U8NjaVJkR

Text Books:

1. Harold Koontz, H. Weihrich, and A.R. Aryasri, Principles of Management, Tata McGraw-Hill, New Delhi, 2004.
2. Essentials of Entrepreneurship and Small Business Management – Norman Scarborough & Jeffrey Cornwall (Pearson, 2016)

References:

1. Innovation & Entrepreneurship – Peter Drucker (Harper, 2006)
2. Entrepreneurship: The Art, Science, and Process for Success – Charles Bamford & Garry Bruton (McGraw-Hill, 2015)
3. Management and Entrepreneurship-NVR Naidu, T Krishna Rao, I.K. International Publishing House Pvt. Ltd.@ 2008
4. Poornima M Charantimath, Entrepreneurship Development and Small Business Enterprises, Pearson Education, 2006.

Course Outcomes (COs):

At the end of the course, student will be able to

1. Plan and organize for the manpower in the given type of organization (PO: 6,9,11)
2. Use staffing Leading and controlling function for the given organization. (PO: 6,8,9,10)
3. Understand the fundamentals of entrepreneurship with the goal of fulfilling the requirements of the industries and holding the responsibilities towards the society. (PO-6,7,8)
4. Design a basic business plan by considering case studies and show the involvement of ownership in Business. (PO-3,7,8,11)
5. Start a new small business with the help of E-Commerce and the current available technologies. (PO-5,11)

CYBER SECURITY ATTACKS AND DEFENSE STRATEGIES	
Course Code: CY62	**Credits: 3:1:0**
Prerequisite: Nil	**Contact Hours: 42L+14T**
Course Coordinator: Mrs. Shankaramma	

Course Contents

Unit I

Security Posture: Current threat landscape, cyber security challenges, enhancing your security posture. **Incident response process**: Handling an incident, post incident activity, incident response in the cloud.

- Pedagogy: Chalk and board, Active Learning, Problem based learning.

Unit II

Understanding the cybersecurity kill chain: External reconnaissance, Access and privilege escalation, exfiltration, sustainment, assault, obfuscation, threat life cycle management. **Reconnaissance**: Internal and external reconnaissance.

- Pedagogy: Chalk and board, Active Learning, Demonstration.

Unit III

Compromising the system: Analysing current trends, phishing, exploiting a vulnerability, zero day, performing the steps to compromise a system. **Chasing a user identity**: Identity is the new perimeter, strategies for compromising a user's identity, hacking a user's identity.

- Pedagogy: Chalk and board, Problem based learning, Demonstration.

Unit IV

Lateral movement: Infiltration, performing lateral movement. **privilege escalation:** infiltration, avoiding alerts, performing privilege escalation, conclusions and lessons learned and summary.

- Pedagogy: Chalk and board, Problem based learning, Demonstration

Unit V

Security Policy: Reviewing security policy, education of the end user, policy enforcement, monitoring for compliance. **Network segmentation:** Defence in depth approach, physical network segmentation, securing remote access to the network, Site-to-Site VPN, virtual network segmentation, Hybrid cloud network security.

- Pedagogy: Chalk and board, Problem based learning, Demonstration.

Tutorial Questions:

1. Portswigger Path Traversal: -This lab contains a path traversal vulnerability in the display of product images.
2. Portswigger sql injection vulnerability allowing login bypass.
3. To build a trojan and know the harm the harm of trojan malware in System.
4. Defeating Malware: Using chkrootkit and Rootkit hunter to defeat malware

5. Using python script to scan the target machine for open ports
6. Create a simple keylogger using python.
7. Using tcdump: Command line Packet Sniffer to sniff the network traffic.
8. Network Scanning and Enumeration: nikto tool for scanning/sniffing
9. Hacking into user's identity: Bruteforce Attack
10. Command Execution using Meterpreter.
11. Automatic Scanning using OWASP ZAP
12. SQL Injection Testing and Data Extraction using SQLmap.
13. Wireless Sniffing/Scanning Tools Aircrack-ng
14. Wireless Sniffing/Scanning using Kismet.

Text Books:

1. Diogenes, Yuri, and Erdal Ozkaya, Cybersecurity–Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals. Packt Publishing Ltd, 2019.
2. Süzen, Ahmet Ali, A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem. International Journal of Computer Network & Information Security 12.1 2020.

References:

1. Bamrara, Dr Atul, Gajendra Singh, and Mamta Bhatt, Cyber-attacks and defense strategies in India: An empirical assessment of the banking sector. Available at SSRN 2488413,2013.

Course Outcomes (COs):

At the end of the course, the student will be able to:

1. Understand cybersecurity skills to protect critical data, networks, and digital assets. (PO 1,2, 3, PSO 1,2,3)
2. Describe the steps to compromise a system, chasing a user identity. (PO 1,2, PSO 1,2)
3. Apply privilege escalation, infiltration and escalation. (PO 1,2, 3, 4, 5, PSO 1,2)
4. Demonstrate security policy, phishing and network segmentation. (PO 1,2, 3, 4, 5, PSO 1,2,3)
5. Analyze cyber security challenges and threat intelligence. (PO 1,2, 3, 5,8 PSO 1,2,3)

Course Assessment and Evaluation:

Continuous Internal Evaluation (CIE): 50 Marks		
Assessment Tools	**Marks**	**Course Outcomes (COs) addressed**
Internal Test-I (CIE-I)	30	CO1, CO2
Internal Test-II CIE-II)	30	CO3, CO4, CO5
Average of the two CIE shall be taken for 30 marks		
Other Components		
Tutorial Assignment 1	10	CO1, CO2, CO3
Tutorial Assignment 2	10	CO4, CO5
The Final CIE out of 50 Marks = Average of two CIE tests for 30 Marks+ Marks scored in Case Study +Marks scored in Assignment		
Semester End Examination (SEE)	50	CO1, CO2, CO3 CO4, CO5

VULNERABILITY ASSESSMENT AND PENETRATION TESTING LABORATORY	
Course Code: CYL65	**Credits: 0:0:1**
Prerequisite: Nil	**Contact Hours: 14P**
Course Coordinator: Mrs. Shankaramma	

Course Contents

PART A

1) a) Imagine you are working as a cybersecurity analyst for a financial institution, you have been assigned the critical task of conducting a Nessus vulnerability analysis on a critical host system (windows, Linux) in the local network hosting sensitive customer data. Detail your step-step approach, including pre-scan preparations, specific Nessus configurations for maximum efficacy in an environment, scan the targets, prioritize and analyse the results and generate reports.

   b) As part of a penetration testing engagement for a client, you're tasked with evaluating the security of their internal network. You suspect that sensitive data might be leaking from one of their development servers due to a potential misconfiguration or a compromised machine within their network. To investigate further, you plan to intercept network traffic using Wireshark to identify any unauthorized data transfers.

2) a) As a member of Blue team experts in Monitoring and Technical Support of a medium sized company, you have been asked to assess the security posture of the internal network. Use Nmap for network discovery, Port scanning, Service version detection and vulnerability detection. Then Document your findings, including the identified vulnerabilities, their severity levels.

   b) Imagine you are a member of Red Team in a company, you have been assigned a penetration testing task to assess the security of a corporate network using Kali Linux and the Metasploit framework. Outline a step-by-step process for utilizing Metasploit to identify and exploit vulnerabilities within the network.

3) Imagine a legal firm handling contracts for clients remotely. Let's say a client, Mr. John, needs to sign a contract for a property purchase. how could Cryptool be applied to digitally sign a contract document, authenticate its validity, and ensure the secure storage of both the digital signature and the original document? Demonstrate the use of digital signatures using Cryptool by performing following things:

   a. Creation of signature
   b. Storing the signature
   c. Verifying the signature

4) Imagine you're a cybersecurity analyst tasked with assessing the security of a newly developed e-commerce website. You would utilize Burp suite and perform following activities to identify and mitigate security flaws in the web application. Start by describing the setup process for

Burp Suite, including configuring proxy settings and initiating automated scans to detect common vulnerabilities like SQL Injection.

a. Manual Testing of SQL Injection
b. Proxy Attack with Burp Suite.

5) Imagine you're a cybersecurity analyst responsible for evaluating the security of a newly launched online education platform. You need to use Burp Suite to find and address any security issues within the application. Explain how you would set up Burp Suite, including configuring the proxy settings and running automated scans to uncover common vulnerabilities.

a. XSS(Cross Site Scripting)
b. CSRF(Cross Site Request Forgery)

6) ABC Corp, a medium-sized company, is concerned about the security of its network and wants to ensure that its employees are using strong passwords. The IT security team has been tasked with conducting a password strength assessment to identify weak passwords that may pose a security risk. The IT security team decides to use a password cracking tool, to perform the password strength assessment. The plan to target the company's internal systems, including FTP, SSH. By using Hydra password cracking tool perform a password strength assessment, so that ABC Corp's IT security team was able to identify and address weaknesses in their network's authentication mechanisms.

7) Imagine you are the network security administrator for a medium-sized e-commerce company that operates an online store handling sensitive customer information. Recently, there have been reports of intermittent service disruptions and slow response times on your company's website, resulting in customer complaints and loss of revenue. After conducting initial investigations, you suspect that the website may be experiencing denial-of-service (DoS) attacks, specifically SYN floods and Ping flood attacks. So, it is important for organizations to have response plans in place to mitigate the impact of DoS attacks on their operations. Use Hping3, kali Linux tool to perform SYN floods and ping flood attacks to launch DOS attack on the target machine and proactively monitor the networks for signs of attack.

8) In a cybersecurity lab environment, a team is tasked with implementing and testing an Intrusion Prevention and Detection System (IDS) using Snort. The team's objectives include configuring Snort for optimal performance, conducting rigorous testing to ensure its effectiveness, and developing custom Snort rules tailored to specific security requirements. Additionally, the team aims to simulate real-world attack scenarios using Kali Linux to detect and mitigate potential threats effectively.

Part B

In VAPT lab, with a maximum of four members per team, engage in collaborative projects focused on assessing and strengthening the security of web applications and networks.

These evaluations entail identifying vulnerabilities, scrutinizing attack surfaces, and executing penetration tests to simulate real-world cyber threats.

At the end in the comprehensive demonstration, teams showcase their findings, methodologies, and recommendations to stakeholders, highlighting their contributions towards fortifying the overall security infrastructure.

Text Book:

1. Messier, Ric, CEH v11 Certified Ethical Hacker Study Guide + Practice Tests Set, 2 nd Edition, November 2021, Wiley & Sons Ltd, ISBN: 978-1-119-82539-5

Course Outcomes (COs):

At the end of the course, student will be able to:

1. Implement techniques for maintaining access and pivoting within a compromised network (PO 1,2,3,5,10 PSO 1,2,3)

2. Perform network discovery using tools and identify potential vulnerabilities. (PO 1,2,3,5,6,8,10 PSO 1,2,3)

3. Conduct various social engineering attacks to assess human vulnerabilities (PO 1,2,3,5,8,10 PSO 1,2,3)

Course Assessment and Evaluation:

Parameter	**Marks**
CIE Test/Project Demo	20
Lab Record Writing + Viva+ program execution	30
Total	**50**
Final Exam will be conducted for 50 marks (SEE)	

CYBER SHIELD LABORATORY	
Course Code: CYL66	**Credits: 0:0:1**
Prerequisite: Nil	**Contact Hours: 14P**
Course Coordinator: Mrs. Shankaramma	

Course Contents

Part A

1. You have received a suspicious binary file. Without running it, identify unique patterns or signatures that could indicate its malware family or type. Use an open source tool to create rules or signatures that can help classify this file among others.
   Tool: YARA
2. Disassemble the suspicious binary and analyse its code flow to determine what actions the malware is programmed to perform. Identify any suspicious API calls or functions it uses that could indicate malicious intent.
   Tool: Ghidra
3. Perform a detailed static analysis of the binary to uncover hidden strings, imports, or embedded resources that can give clues about the malware's purpose or communication methods.
   Tool: Radare2
4. Execute the malware sample safely within a controlled environment to observe and log its runtime behaviour. Record changes it makes to the file system, registry, and any new processes it spawns. Capture network activity during execution.
   Tool: Cuckoo Sandbox
5. Analyze the captured network traffic from the malware execution to identify potential command and control (C2) communications or data exfiltration attempts. Extract indicators of compromise such as IP addresses or domain names.
   Tool: Wireshark

Part B

6. Set up a host-based intrusion detection system that monitors logs and file integrity to detect suspicious activity or rootkits. Configure it to generate alerts.
7. Deploy an open source antivirus solution to scan your system for known malware signatures and clean infections. Test scanning suspicious files.
8. Configure a tool to monitor login/authentication attempts and automatically ban IPs that fail repeatedly to prevent brute force attacks.
9. Implement system-wide event monitoring on Windows to track process creations, network connections, and file modifications in real time. Use this data to detect anomalous activity.
10. Set up a network intrusion detection system to analyse network traffic for malware-related signatures and generate alerts on suspicious activity

Text Books:

1. "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" by Michael Sikorski and Andrew Honig, 2012.
2. "Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code" by Michael Ligh, Steven Adair, Blake Hartstein, and Matthew Richard, 2010.

Reference Books:

1. "The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory" by Michael Hale Ligh, Andrew Case, Jamie Levy, and AAron Walters, 2014

2. "Network Intrusion Detection" by Stephen Northcutt and Judy Novak, 2002.

Course Outcomes (COs):

At the end of the course, the student should be able to:

1. Perform static and dynamic malware analysis using open source tools to identify malicious code and behaviours. (PO-1,2,4,5,10, PSO-1,2)
2. Deploy and configure malware detection and prevention tools including intrusion detection systems and antivirus software. (PO-1,2,5,8,10, PSO-1,2,3)
3. Analyze system and network logs to detect suspicious activities and potential security breaches. (PO-1,2,4,5,8,10, PSO-1,2,3)

Course Assessment and Evaluation:

Parameter	**Marks**
CIE Test	20
Lab Record Writing + Viva+ program execution	30
Total	**50**
Final Exam will be conducted for 50 marks (SEE)	

MALWARE ANALYSIS	
Course Code: CYE631	**Credits: 3:0:0**
Prerequisite: Nil	**Contact Hours: 42L**
Course Coordinator: Mrs. Shankaramma	

Course Contents

Unit I

Introduction to Malware Analysis: What is Malware? What is Malware Analysis? Why is Malware Analysis? Types of Malware Analysis. **Static Analysis**: Determining the File Type, Fingerprinting the Malware, Multiple Anti-Virus Scanning, Extracting Strings, Determining File Obfuscation.

- Pedagogy: Chalk and board, Problem based learning, Demonstration.

Unit II

Inspecting PE Header Information, Comparing and Classifying The malware. **Dynamic Analysis:** System And Network Monitoring, Dynamic Analysis (Monitoring) Tools, Dynamic Analysis Steps, Putting it All Together: Analyzing a Malware Executable, Dynamic Link Library (DLL) Analysis.

- Pedagogy: Chalk and board, Problem based learning, Demonstration.

Unit III

Disassembly Using IDA: Code Analysis Tools, Static Code Analysis (Disassembly) Using IDA, Disassembling Windows API, Patch Binary Using IDA, IDA Scripting and Plugins, **Code Injection and Hooking:** Virtual Memory, User Mode and Kernal Mode.

- Pedagogy: Chalk and board, Problem based learning, Demonstration.

Unit IV

Code Injection Techniques, Hooking Techniques**. Malware Obfuscation Techniques:** Simple Encoding, Malware Encryption, Custom Encoding/ Encryption, Malware Unpacking. **Hunting Malware Using Memory Forensics:** Memory Forensic Steps, Memory Acquisition.

- Pedagogy: Chalk and board, Problem based learning, Demonstration.

Unit V

Enumerating Processes, Listing DLLs, Dumping an Executable and DLL**, Detecting Advanced Malware Using Memory Forensics:** Detecting Code Injection, Investigating Hollow Process Injection, Detecting API Hooks, I/O Processing, Displaying Device Trees, Determine Kernel Space Hooking, Kernel Callbacks and Timers.

- Pedagogy: Chalk and board, Problem based learning, Demonstration.

Text Book:

1. Monnappa K A, Learning Malware Analysis, Packt Publishing Ltd, 2018..

Reference Book:

1. Michael Sikorski and Andrew Honig, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software‖, No Starch Press, 2012

Course Outcomes (COs):

At the end of the course, the students should be able to:

1. Understand the fundamentals of malware, types of malware, and techniques for static malware analysis. (PO-1,2,PSO-1)
2. Demonstrate dynamic malware analysis using system and network monitoring tools and analyze executable files and DLLs. (PO-1,2,4,5, PSO-1,2)
3. Discuss the principles of static code analysis, hooking and code injection. (PO-1,2,4,5, PSO-1,2)
4. Describe malware obfuscation, encoding/encryption, unpacking, and memory forensic techniques.(PO-1,2,4, PSO-1,2)
5. Explain memory forensic techniques to detect advanced malware behavior and kernel-level attacks.(PO-1,2,4, PSO-1,2)

Course Assessment and Evaluation:

Continuous Internal Evaluation (CIE): 50 Marks		
Assessment Tools	**Marks**	**Course Outcomes (COs) addressed**
Internal Test-I (CIE-I)	30	CO1, CO2
Internal Test-II CIE-II)	30	CO3, CO4, CO5
Average of the two CIE shall be taken for 30 marks		
Other Components		
Case study	10	CO1, CO2, CO3
Assignment	10	CO4, CO5
The Final CIE out of 50 Marks = Average of two CIE tests for 30 Marks+ Marks scored in Case Study +Marks scored in Assignment		
Semester End Examination (SEE)	50	CO1, CO2, CO3 CO4, CO5

CYBER THREAT INTELLIGENCE	
Course Code: CYE632	**Credits: 3:0:0**
Prerequisite: Nil	**Contact Hours: 42L**
Course Coordinator: Mrs. Shankaramma	

Course Contents

Unit I

Introduction to Threat Intelligence: What is Threat Intelligence? What have you heard about threat Intelligence? Why is Threat Intelligence is important? Who can benefit from Threat Intelligence, Data and information are not intelligence, Two types of Threat Intelligence, The Role of Threat Data Feeds, The Role of Private Channels and the Dark Web**? Threat Intelligence Lifecycle:** The Six Phases of the Threat, Intelligence Lifecycle, Tools and People.

- Pedagogy: Chalk and board, Problem based learning.

Unit II

Threat Intelligence for Security Operations: Responsibilities of the SOC Team, The Overwhelming Volume of Alerts, Use case: Correlating and enriching alerts. **Threat Intelligence for Incident response:** Continuing Challenges, The Reactivity Problem, Minimizing Reactivity in Incident Response, Strengthening Incident Response with Threat, Intelligence, Threat Intelligence in Action, Essential Characteristics of Threat Intelligence for Incident Response. **Threat Intelligence for Vulnerability Management:** The Vulnerability Problem by the Numbers, Assess Risk Based on Exploitability.

- Pedagogy: Chalk and board, Problem based learning.

Unit III

The Genesis of Threat Intelligence: Vulnerability Databases, Threat Intelligence and Real Risk, Sources of Intelligence, Use Case: Cross-Referencing Intelligence. **Threat Intelligence for Security Leaders:** Risk Management, Mitigation, Investment, Communication, Supporting Security Leaders, The Security Skills Gap, Intelligence to Manage Better. **Threat Intelligence for Risk Analysis**: A Fair Risk Model, **Threat Intelligence for Fraud Prevention:** Stand and Deliver, Know Your Enemy, Criminal Communities and the Dark Web, Connecting the Dots for Fraud Prevention. Use cases: Payment fraud, Compromised data, Typo-squatting and fraudulent domains.

- Pedagogy: Chalk and board, Problem based learning.

Unit IV

Threat Intelligence for Reducing Third Party Risk: Third-Party Risk Looms Large, Traditional Risk Assessments Fall Short, Three Things to Look for in Threat Intelligence, Responding to High Third-Party Risk Scores. **Threat intelligence for Digital Risk Protection**: Being Online ids Being at Risk, Types of Digital Risk, Uncovering Evidence of breaches on the Web. **Analytical Frameworks for Threat Intelligence**: The Lockheed Martin Cyber Kill Chain, The Diamond Model, The MITRE ATT & CK Framework.

- Pedagogy: Chalk and board, Problem based learning.

Unit V

Threat Intelligence journey: Threat Intelligence Needs and Goals, Key Success Factors, Start Simple and Scale Up. **Developing the core threat intelligence Team: Dedicated** teams, Core Competencies, Collecting and Enriching Threat Data, Engaging with Threat Intelligence Communities, Conclusion: Moving Toward a Security Intelligence Program.

- Pedagogy: Chalk and board, Problem based learning.

Text Books:

1. Christoper Ahlberg, The Threat Intelligence Handbook Second edition, Zane Pokorny CyberEdge Press, 2019.

References:

1. Dehghantanha, Ali, Mauro Conti, and Tooska Dargahi, Cyber threat intelligence, New York, NY: Springer International Publishing, 2018.
2. Roberts, Scott J., and Rebekah Brown, Intelligence-driven incident response: Outwitting the adversary, O'Reilly Media, 2017.

Course Outcomes (COs):

At the end of the course, the students should be able to:

1. Understand the genesis and fundamentals of cyber threat intelligence, and process of managing cyber threats. (PO 1,2,3 PSO 1,3)
2. Explain vulnerability management and security incident response process. (PO 1,2,3, PSO 1,2)
3. Perform security risks analysis using various risk analysis tools. (PO 1,2, 4,5, PSO 1,2)
4. Apply threat intelligence to assess and manage internal and third-party security risks. (PO 1,2,5,8, PSO 1,3)
5. Apply the principles of threat intelligence to define organizational needs and goals (PO 1,2,4, 9, PSO 1,2)

Course Assessment and Evaluation:

Continuous Internal Evaluation (CIE): 50 Marks		
Assessment Tools	**Marks**	**Course Outcomes (COs) addressed**
Internal Test-I (CIE-I)	30	CO1, CO2
Internal Test-II CIE-II)	30	CO3, CO4, CO5
Average of the two CIE shall be taken for 30 marks		
Other Components		
Case study	10	CO1, CO2, CO3
Assignment	10	CO4, CO5
The Final CIE out of 50 Marks = Average of two CIE tests for 30 Marks+ Marks scored in Case Study +Marks scored in Assignment		
Semester End Examination (SEE)	50	CO1, CO2, CO3 CO4, CO5

SECURE SOFTWARE DEVELOPMENT LIFE CYCLE	
Course Code: CYE633	**Credits: 3:0:0**
Prerequisite: Nil	**Contact Hours: 42L**
Course Coordinator: Dr. Nayana G. Bhat	

Course Contents

Unit I

SSDLC Overview: Introduction, need for secure SDLC, security basics, common threats, CIAAA model, shift-left security, frameworks (OWASP/SAMM, NIST SSDF).

- Pedagogy: Chalk and board, Problem based learning.

Unit II

Security Requirements & Planning: Requirement engineering for security, threat modeling (STRIDE, DREAD), security policy decomposition, use/misuse case modeling

- Pedagogy: Chalk and board, Problem based learning.

Unit III

Secure Design: Secure design principles, architecture risk analysis, design patterns, secure technologies, access control, secure APIs, data validation

- Pedagogy: Chalk and board, Problem based learning.

Unit IV

Secure Implementation: Secure coding standards (OSWAP Top Ten, CERT), code analysis (SAST, DAST), version control (Git), secure CI/CD, **Security Testing:** Security test plan, fuzz testing, penetration testing, vulnerability scanning, dynamic/static analysis, bug tracking, code review rubrics.

- Pedagogy: Chalk and board, Problem based learning.

Unit V

Deployment, Operations & Maintenance: Secure deployment, patch management, secure DevOps, monitoring/logging, incident response, supply chain security.

- Pedagogy: Chalk and board, Problem based learning.

Textbooks:

1. Secure Software Development Life Cycle (SSDLC): From Planning to Deployment: A Comprehensive Guide to Building Secure Software Applications (The Cyber Security Series Book 2) by Malik Shah Jahan.

References:

1. Art of Software Security Assessment, The: Identifying and Preventing Software Vulnerabilities, 2006.
2. Building Secure Software: How to Avoid Security Problems the Right Way, John Viega (Author), Gary McGraw, 2011.

Course Outcomes (COs):

At the end of the course, students will be able to:

1. Explain SSDLC phases, secure coding standards, and security frameworks. (PO-1,3, PSO-1)
2. Identify and model software threats, vulnerabilities, and requirements for secure engineering. (PO-1,2,3, PSO-1)
3. Discuss security controls in software design, development, and deployment.(PO-1,2,3, PSO-1)
4. Understand security testing, code reviews and vulnerability assessment. (PO-1,2,3, PSO-1)
5. Analyze security, privacy, and legal implications of software systems. (PO-1,2,3,8, PSO-2,3)

Course Assessment and Evaluation:

Continuous Internal Evaluation (CIE): 50 Marks		
Assessment Tools	**Marks**	**Course Outcomes (COs) addressed**
Internal Test-I (CIE-I)	30	CO1, CO2
Internal Test-II CIE-II)	30	CO3, CO4, CO5
Average of the two CIE shall be taken for 30 marks		
Other Components		
Case study	10	CO1, CO2, CO3
Assignment	10	CO4, CO5
The Final CIE out of 50 Marks = Average of two CIE tests for 30 Marks+ Marks scored in Case Study +Marks scored in Assignment		
Semester End Examination (SEE)	50	CO1, CO2, CO3 CO4, CO5

WEB APPLICATION SECURITY	
Course Code: CYE634	**Credits: 3:0:0**
Prerequisite: Nil	**Contact Hours: 42L**
Course Coordinator: Dr. Sahana Lokesh R	

Course Content

Unit 1

Fundamentals of Web Application Security: The history of Software Security-Recognizing Web Application Security Threats, Web Application Security, Authentication and Authorization, Secure Socket layer, Transport layer Security, Session Management-Input Validation

- Pedagogy: Chalk and board, Problem based learning.

Unit 2

Secure Development and Deployment: Web Applications Security – Security Testing, Security Incident Response Planning, The Microsoft Security Development Lifecycle (SDL), OWASP Comprehensive Lightweight Application Security Process (CLASP), The Software Assurance Maturity Model (SAMM)

- Pedagogy: Chalk and board, Problem based learning.

Unit 3

Vulnerability Assessment and Penetration Testing: Vulnerability Assessment Lifecycle, Vulnerability Assessment Tools: Cloud-based vulnerability scanners, Host-based vulnerability scanners, Network-based vulnerability scanners, Databasebased vulnerability scanners, Types of Penetration Tests: External Testing, Web Application Testing, Internal Penetration Testing, SSID or Wireless Testing, Mobile Application Testing.

- Pedagogy: Chalk and board, Problem based learning.

Unit 4

Hacking Techniques and Tools: Social Engineering, Injection, Cross-Site Scripting(XSS), Broken Authentication and Session Management, Cross-Site Request Forgery, Security Misconfiguration, Insecure Cryptographic Storage, Failure to Restrict URL Access, Tools: Comodo, OpenVAS, Nexpose, Nikto, Burp Suite, etc.

- Pedagogy: Chalk and board, Problem based learning.

Unit 5

Browser Security Principles: Origin Policy - Exceptions to the Same-Origin Policy - Cross-Site Scripting and Cross-Site Request Forgery - Reflected XSS - HTML Injection

- Pedagogy: Chalk and board, Problem based learning.

Text Books:

1. Andrew Hoffman, Web Application Security: Exploitation and Countermeasures for Modern Web Applications, First Edition, 2020, O'Reilly Media, Inc.

2. Bryan Sullivan, Vincent Liu, Web Application Security: A Beginners Guide, 2012, The McGraw-Hill Companies.

Reference Books:

1. Michael Cross, Developer's Guide to Web Application Security, 2007, Syngress Publishing, Inc.
2. Ravi Das and Greg Johnson, Testing and Securing Web Applications, 2021, Taylor & Francis Group, LLC.

Course outcome:

At the end of the course the student will be able to:

1. Understand concepts of threats and secure practices for web applications.(PO-1,2,3,PSO-1)
2. Discuss different deployment standards for building secure web applications..(PO-1,2,3,PSO-1,2)
3. Demonstrate vulnerability assessments using various tools and techniques, and perform different types of penetration tests..(PO-1,2,3,5,PSO-1,2)
4. Identify and mitigate common web vulnerabilities and attacks.(PO-1,2,3,5,PSO-1,2)
5. Analyze browser security mechanisms and vulnerabilities.(PO-1,2,3,5,PSO-1,2)

Course Assessment and Evaluation:

Continuous Internal Evaluation (CIE): 50 Marks		
Assessment Tools	**Marks**	**Course Outcomes (COs) addressed**
Internal Test-I (CIE-I)	30	CO1, CO2
Internal Test-II CIE-II)	30	CO3, CO4, CO5
Average of the two CIE shall be taken for 30 marks		
Other Components		
Case study	10	CO1, CO2, CO3
Assignment	10	CO4, CO5
The Final CIE out of 50 Marks = Average of two CIE tests for 30 Marks+ Marks scored in Case Study +Marks scored in Assignment		
Semester End Examination (SEE)	50	CO1, CO2, CO3 CO4, CO5

PRIVACY MANAGEMENT	
Course Code: CYE635	**Credits: 3:0:0**
Prerequisite: Nil	**Contact Hours: 42L**
Course Coordinator: Dr.Vishalakshi Prabhu H	

Course Contents

Unit I

Introduction to cyber security: Critical characteristics of Information, CNSS security model, CIA triangle, Components of an Information System, Security Systems Development Life Cycle, Security Professionals and the Organization

Legal, Ethical and Professional issues in Information Security: Laws and ethics, International laws and legal bodies, Ethics and Information Security, Codes of ethics and professional organizations

- Pedagogy: Chalk and board, Problem based learning, Interactive Demo
- Link: https://nptel.ac.in/courses/106106248

Unit II

Risk management: Overview, Risk Identification, Risk Assessment, Risk Control strategies

Planning for security: Information Security Policy, Standards and Practices (EISP, ISSP, SysSP), Policy management, Information Security Blueprint, Continuing strategies

- Pedagogy: Chalk and board, Problem based learning, Interactive Demo
- Link: https://nptel.ac.in/courses/106106248

Unit III

Security technology: Introduction, Access control, Firewalls (modes, categories, generation, architecture, configuring), IDPS (Terminology, types, detection methods), Scanning and analysis tools, Biometric Access Controls

- Pedagogy: Chalk and board, Problem based learning, Interactive Demo
- Link: https://nptel.ac.in/courses/106106248

Unit IV

Information Security project management: Conversion strategies, Bulls Eye model, certification vs accreditation

Security and personnel: Positioning and staffing the security function, qualifications, Credentials of Information Security professionals

- Pedagogy: Chalk and board, Problem based learning, Interactive Demo
- Link: https://nptel.ac.in/courses/106106248

Unit V

Privacy regulation: In Europe (GDPR); Privacy: The Indian Way, DPDP, Aadhar;

Information privacy: Economics and strategy, Economic value of privacy, privacy valuation, WTA and WTC, Business strategy and privacy, espionage, Privacy vs safety

- Pedagogy: Chalk and board, Problem based learning, Interactive Demo
- Link: https://nptel.ac.in/courses/106106248

Text Books:

1. Principles of Information Security by Michael E. Whitman and Herbert J. Mattord (6th edition, Cengage Learning, India)

2. Privacy 3.0: Unlocking Our Data-Driven Future, Rahul Matthan, ISBN: 9789362130747, May 2024

References:

1. Security, Privacy, and Anonymization in Social Networks: Emerging Research and Opportunities, B. K. Tripathy & Kiran Baktha, IGI Global, 2018, ISBN**:** 978-1-5225-5158-4

Course outcomes (Cos):

At the end of the course the student will be able to:

1. Understand the principles of information security, CIA triad, ethics and security governance frameworks. (PO-1,2,3,8 PSO:1,2,3)
2. Analyze the role of policies/standards in establishing effective security programs. (PO-1,2,3,8, PSO:1,2,3)
3. Apply appropriate security technologies, access control mechanisms, and cryptography to protect data. (PO-1,2,3,5, PSO:1,2,3)
4. Demonstrate privacy-compliant information systems and ethical standards. (PO-1,2,3,8 PSO:1,2,3)
5. Describe different privacy and data protection regulations.(PO-1,2,3,8 PSO:1,2,3)

Course Assessment and Evaluation:

Continuous Internal Evaluation (CIE): 50 Marks		
Assessment Tools	**Marks**	**Course Outcomes (COs) addressed**
Internal Test-I (CIE-I)	30	CO1, CO2
Internal Test-II CIE-II)	30	CO3, CO4, CO5
Average of the two CIE shall be taken for 30 marks		
Other Components		
Case study	10	CO2, CO3, CO4
Assignment	10	CO1, CO5
The Final CIE out of 50 Marks = Average of two CIE tests for 30 Marks+ Marks scored in Case Study +Marks scored in Assignment		
Semester End Examination (SEE)	50	CO1, CO2, CO3 CO4, CO5

DEEP LEARNING	
Course Code: CYE641	**Credits: 3:0:0**
Prerequisite: Nil	**Contact Hours: 42L**
Course Coordinator: Dr. A N Ramya Shree	

Course Contents

Unit I

Introduction to Deep Learning: Significance of weights and bias, Working of a single neuron, Working of a layer, layer implementation with NumPy, dense layer, sigmoid, ReLU, tanh, and softmax activation functions.

- Pedagogy: Chalk and board, Power point presentations.

Unit II

Loss Function: Categorical cross entropy loss, binary cross entropy loss, and accuracy calculation. Backpropagation Algorithm, Optimizers: Stochastic Gradient Descent (SGD), Learning Rate and LR Decay, SGD with Momentum, AdaGrad, RMSProp, Adam.

- Pedagogy: Chalk and board, Power point presentations.

Unit III

Convolutional Neural Networks: Key components of CNN, the convolution operation, convolution with and without kernel flipping, pooling, sparse interactions, parameter sharing, equivariant representations, LeNet, AlexNet, and ResNet CNN architectures.

- Pedagogy: Chalk and board, Power point presentations.

Unit IV

Recurrent Neural Networks: Unfolding Computational Graphs, Teacher Training Force, Recurrent Neural Network, Backpropagation through Time (BPTT), Bidirectional RNNs, Long Short-Term Memory, and Gated Recurrent Neural Network.

- Pedagogy: Chalk and board, Power point presentations.

Unit V

Transformers : Self-attention and multi-head attention mechanisms, positional encoding, residual connection, layer normalization, transformer architecture, encoder and decoder applications.

- Pedagogy: Chalk and board, Power point presentations.

Text Books:

1. Harrison Kinsley & Daniel Kukiela, Neural Network from Scratch in Python, Kinsley Enterprises Inc., MIT license, 2020.
2. Ian Goodfellow, Yoshua Bengio, Aaron Courville, Deep Learning, MIT Press, 2016.
3. Denis Rothman, Transformers for Natural Language Processing, Packt, 2e, March 2022

References:

1. Bengio, Yoshua. Learning deep architectures for AI. Foundations and trends in Machine Learning, 2009.
2. Nikhil Buduma, Fundamentals of Deep Learning: Designing Next-Generation Machine Intelligence Algorithms, O'Reilly Publications 2022.

.

Course Outcomes (COs):

At the end of the course, students will be able to:

1. Understand the fundamentals of deep learning, role of weights, biases, neurons and layers, and activation functions.(PO 1,2,3,4,5,6,12 PSO 1,2).
2. Demonstrate loss functions ,cross-entropy, backpropagation algorithm and optimization techniques . (PO 1,2,3,4,5,6,12 PSO 1,2)
3. Apply deep feed forward networks and convolutional neural networks to solve real time problems. (PO 1,2,3,4,5,6,12 ,PSO 1,2,3)
4. Demonstrate the working of recurrent neural network functions. (PO 1,2,3,4,5,6,12 PSO 1,2)
5. Describe the transformer architecture and explore applications of encoder-decoder models in deep learning.(PO 1,2,3,4,5,6,12 PSO 1,2)

Course Assessment and Evaluation:

Continuous Internal Evaluation: 50 Marks		
Assessment Tool	**Marks**	**Course outcomes addressed**
Internal test-I	30	CO1, CO2, CO3
Internal test-II	30	CO3, CO4, CO5
Average of the two internal tests shall be taken for 30 marks.		
Other components		
Assignment	10	CO1, CO2, CO3
Case Study	10	CO1, CO2, CO3, CO4, CO5
Semester End Examination (SEE)	100	CO1, CO2, CO3, CO4, CO5

BIG DATA SYSTEMS	
Course Code: CYE642	**Credits: 3:0:0**
Prerequisite: Nil	**Contact Hours: 42L**
Course Coordinator: Dr. Siddesh G M	

Course Contents

Unit I

Introduction to Big Data: Types of Digital Data, Introduction to Big Data: Characteristics, Evolution, Definition, Challenges, What is Big Data, Other Characteristics, Why Big data, Significance of Big Data, Traditional BI versus Big Data, Data warehouse environment versus Hadoop Environment, Trends in Big data, Big Data Analytics: Introduction to Big Data Analytics, Classification of Analytics, Importance of Big Data Analytics, Technologies for Big data, Data Science, Data Scientist, Terminologies Used.

- Pedagogy: Chalk and board, Power point presentations.

Unit II

Hadoop / Spark /HDFS Overview: Hadoop Overview: Features, Key advantages, Versions, Distributions, Overview of Hadoop Ecosystem, Why Hadoop, why not RDBMS, HDFS: Hadoop Distributed File System (HDFS), HDFS Daemons, File Read, File Write, Replica Placement Strategy, HDFS commands, Special features of HDFS and its limitations, MapReduce, YARN.

- Pedagogy: Chalk and board, Power point presentations.

Unit III

Spark Core: Spark Overview: Spark Ecosystems, Advantages of Spark, Spark Standalone application, Running on Cluster, Programming with RDD's: Basics, RDD operations, Lineage Graphs, Lazy evaluation, Persistence, Immutability, Fault Tolerance, Performance (Pipelining, Shuffle). Pair RDD's: Transformations and Actions, Partitioning, Accumulators, Broadcast Variables.

- Pedagogy: Chalk and board, Power point presentations.

Unit IV

Spark SQL: Rows, Data frames, Tables and SQL operations on Tables. Spark Session, Creating Data Frame, Parquet files, working with Hive. Spark Streaming: Introduction to Stream Processing, Architecture of Spark Streaming, Caching and Persistence, Check pointing, Fault tolerance, Structured Streaming-Output Modes, Output sinks, Failure recovery and check pointing.

- Pedagogy: Chalk and board, Power point presentations.

Unit V

Machine Learning with Spark: Introduction to spark ML Lib, need for pipeline API, working of pipeline API, Scala syntax for building pipeline, Predictions on test documents, Feature engineering, Feature extraction algorithms, Feature transformation algorithms, Feature selection algorithms, classification and regression, clustering, Collaborative filtering, ML-tuning - model selection and hyperparameter tuning

- Pedagogy: Chalk and board, Power point presentations.

Text Book:

1. Seema Acharya and Subhashini C, Big Data and Analytics, Wiley India, 2019 (Chapter 1,2,3,5,9)
2. Muhammad Asif Abbasi, Learning Apache Spark 2, Packt Publishing, 2017 (Chapter 1,2,3,4,5,6)

References:

1. Cay S. Horstmann, Scala for the Impatient 2nd Edition (Chapter 1to 6, 12 to 14)
2. Andy Konwinski, Holden Karau, Matei Zaharia, Patrick Wendell, Learning Spark LightningFast Big Data Analysis, O'Reilly, 2015 (Chapter 1, 2, 3, 4, 6, 7, 8, 9,10)
3. Tom White, Hadoop: The Definitive Guide, O'Reilly, 2015

Course Outcomes (COs):

At the end of the course, students will be able to:

1. Understand the Big Data concepts and differentiate Big Data environments from traditional BI systems.(PO-1,2,3, PSO-1,2)

2. Demonstrate Hadoop ecosystem tools including HDFS, MapReduce, and YARN for large-scale data processing. (PO-1,2,3,5, 10, PSO-1,2)

3. Explain the various components of Spark architecture and their key features.(PO-1,2,3, PSO-1,2)

4. Implement RDD operations, data processing with Spark SQL and Spark Streaming for batch and real-time analytics. (PO-1,2,3,5,10, PSO-1,2)

5. Apply Spark MLlib for machine learning tasks.(PO-1,2,3,5, 10, PSO-1,2)

Course Assessment and Evaluation:

Continuous Internal Evaluation: 50 Marks		
Assessment Tool	**Marks**	**Course outcomes addressed**
Internal test-I	30	CO1, CO2, CO3
Internal test-II	30	CO3, CO4, CO5
Average of the two internal tests shall be taken for 30 marks.		
Other components		
Case study	10	CO1, CO2, CO3
Assignment	10	CO4, CO5
Semester End Examination (SEE)	100	CO1, CO2, CO3, CO4, CO5

PARALLEL COMPUTING	
Course Code: CYE643	**Credits: 3:0:0**
Prerequisite: Nil	**Contact Hours: 42L**
Course Coordinator: Dr. Siddesh G M	

Course Contents

Unit I

A Short History of Supercomputing: Von Neumann Architecture, Cray, multinode computing, nvidia and cuda, alternatives to cuda, types of parallelism.

- Pedagogy / Course delivery tools: Chalk and talk, Power Point Presentation, Videos

Unit II

GPUs History of GPU Computing: FLYNN'S TAXONOMY, SOME COMMON PARALLEL PATTERNS, Reduced Instruction Set Computers, Multiple Core Processors, Vector Processors, Limits to parallelizability, Amdahl's law on Parallelism.

- Pedagogy/Course delivery tools: Chalk and talk, Power Point Presentation, Videos

Unit III

Shared-memory programming with OpenMP **–** openmp pragmas and directives**,** the trapezoidal rule, Scope of variables, the reduction clause, loop carried dependency, scheduling, producers and consumers, Caches, cache coherence and false sharing in openmp, tasking, tasking, thread safety

- Pedagogy/Course delivery tools: Chalk and talk, Power Point Presentation, Videos

Unit IV

Introduction: GPUs as Parallel Computers, Architecture of a Model GPU, Why More Speed or Parallelism? GPU Computing. Introduction to CUDA: Data Parallelism, CUDA Program Structure, A Vector Addition Kernel, Device Global Memory and Data Transfer, Kernel Functions and Threading.

- Pedagogy/Course delivery tools: Chalk and talk, Power Point Presentation, Videos.

Unit V

CUDA Threads: CUDA Thread Organization, Mapping Threads to Multidimensional Data
Implementation of algorithms in CUDA: A Matrix-Matrix Multiplication, Program to implement sorting using CUDA, Program to Histogram calculation using CUDA, Program to create threads using default stream in CUDA, CUDA for Deep Learning - A Case Study.

- Pedagogy/Course delivery tools: Chalk and talk, Power Point Presentation, Videos.

Text Books:

1. Introduction to parallel computing by Ananth Grama, Pearson education Publishers, second edition, 2003.
2. CUDA Programming: A Developer's Guide to Parallel Computing with GPUs, Shane Cook Morgan Kaufmann, 2013, ISBN: 978-0-12-415933-4
3. Peter S Pacheco, Matthew Malensek – An Introduction to Parallel Programming, second edition, Morgan Kauffman
4. Michael J Quinn – Parallel Programming in C with MPI and OpenMp, McGrawHill

References:

1. GPU parallel program development using CUDA by Tolga Soyata. CRC Press 2018.

Course Outcomes (COs):

At the end of the course, students will be able to:

1. Understand the technologies and architectures used for parallel computing. (PO-1,2, PSO-1)
2. Describe Flynn's taxonomy and GPU architecture. (PO-1,2,3 PSO-1)
3. Apply OpenMP pragmas and directives to parallelize programs on shared-memory architectures. (PO-1,2,3,5, PSO-1)
4. Analyse the structure and functionalities of CUDA Programming (PO-1,2,3, PSO-1).
5. Develop multi-threaded applications using CUDA (PO-1,2,3,4,5 , PSO-1)

Course Assessment and Evaluation:

Continuous Internal Evaluation: 50 Marks		
Assessment Tool	**Marks**	**Course outcomes addressed**
Internal test-I	30	CO1, CO2, CO3
Internal test-II	30	CO3, CO4, CO5
Average of the two internal tests shall be taken for 30 marks.		
Other components		
Assignment 1	10	CO1, CO2, CO3
Assignment 2	10	CO1, CO2, CO3, CO4, CO5
Semester End Examination (SEE)	100	CO1, CO2, CO3, CO4, CO5

FULL STACK DEVELOPMENT	
Course Code: CYE644	**Credits: 3:0:0**
Prerequisite: Nil	**Contact Hours: 42L**
Course Coordinator: Mr Subash N /Ms. Veena N	

Course Contents

Unit I

Introduction to Full Stack Development: Client-server Architecture Static vs Dynamic websites Roles and responsibilities How front-end and back-end communicate Introduction, Cascading Styles Sheet: Concept of CS, Creating Style Sheet, CSS Properties, CSS Styling (Background, Text Format, Controlling Fonts), CSS Id and Class, Box Model (Border, Padding, Margin properties), CSS Advanced (Grouping, Dimension, Display, Positioning, Floating, Align, Pseudo class)

- Pedagogy: Chalk and board, Power point presentations.

UNIT II

Front-End Web Development: JavaScript syntax, Types of Data and Variables, Operations and calculations, The Document Object, Using Events. JavaScript Advanced: Scopes and Closures, understand "this" and prototypes, OOps concepts as applied to JS and prototypal inheritance, Understanding the meaning of asynchronous. Event loops, Promises.

- Pedagogy: Chalk and board, Power point presentations.

UNIT III

ReactJS: Building blocks of React, Create-react-app - Create first React app using this CLI, JSX - Understand what it is and how it's required to create components, Simple functional components, CSS - Load CSS and use it via class Name, props - Passing props to components to make them reusable

- Pedagogy: Chalk and board, Power point presentations.

UNIT IV

Back-End Web Development: Node.js: Introduction - What is Node.js, Architecture, Feature of Node JS, Installation and setup - Creating webservers with HTTP (Request & Response), Understand dependence management: npm and package.json File system APIs.CRUD Operations using Node.js: Event Handling - GET & POST implementation, Use Express.js to create a REST API. Use GET, POST

- Pedagogy: Chalk and board, Power point presentations.

UNIT V

Database Integration: Overview of NoSQL vs SQL Document-oriented database model Key features of MongoDB MongoDB Atlas (cloud setup) Core MongoDB Operations (CRUD) Schema Design & Data Modeling Mongoose ODM (Object Data Modeling) Connect to NoSQL MongoDB Database using Node.js, Implementation of CRUD operations.

- Pedagogy: Chalk and board, Power point presentations.

Text Books:

1. Steven A. Gabarro, "Web Application Design and Implementation: Apache 2,PHP5, MySQL, JavaScript, and Linux/UNIX", Wiley- IEEE Computer SocietyPress 2007.
2. Nate Murray, Felipe Coury, Ari Lerner and Carlos Taborda, "Ng-book, The Complete Book on Angular", Fullstack.IO, 1st edition, 2016.
3. KrasimirTsonev, "Node.js by Example", Packt Publishing Limited, 2015

Reference Links:

1. Web link for Node.js: https://nodejs.org/en/
2. Web link for MongoDB: https://www.mongodb.com/
3. https://reactjs.org/:

Course Outcomes (COs):

At the end of the course, students will be able to:

1. Understand the client-server architecture and design responsive web pages using CSS styling techniques. (PO-1,2,3,5, PSO-1,2)
2. Develop interactive front-end applications using JavaScript and object-oriented features. (PO-1,2,3,5, PSO-1,2)
3. Implement reusable user interfaces using ReactJS by leveraging components, JSX, props, and event-driven programming. (PO-1,2,3,5, PSO-1,2)
4. Demonstrate server-side functionality using Node.js by creating web servers and HTTP requests. (PO-1,2,3,5, PSO-1,2)
5. Integrate NoSQL databases and perform CRUD operations for full-stack applications (PO-1,2,3,5, PSO-1,2)

Course Assessment and Evaluation:

Continuous Internal Evaluation (CIE): 50 Marks		
Assessment Tools	**Marks**	**Course Outcomes (COs) addressed**
Internal Test-I (CIE-I)	30	CO1, CO2
Internal Test-II CIE-II)	30	CO3, CO4, CO5
Average of the two CIE shall be taken for 30 marks		
Other Components		
Case study	10	CO1, CO2, CO3
Assignment/Quiz	10	CO4, CO5
The Final CIE out of 50 Marks = Average of two CIE tests for 30 Marks+ Marks scored in Case Study +Marks scored in Assignment		
Semester End Examination (SEE)	50	CO1, CO2, CO3 CO4, CO5

QUANTUM COMPUTING	
Course Code: CYE645	**Credits: 3:0:0**
Prerequisite: Nil	**Contact Hours: 42L**
Course Coordinator: Dr. Anjaneyulu Pasala/ Ms. Veena S	

Course Contents

UNIT I

Fundamentals of Quantum Computing: Overview of Quantum vs. Classical Computing, Basic Concepts in Quantum Mechanics: Superposition, Entanglement, Measurement, Qubits and the Bloch Sphere. Introduction to Quantum Gates: Pauli Gates, Hadamard Gate, Phase Shift, and CNOT, Quantum Circuit Design and Simulation.

- Pedagogy/Course delivery tools: Chalk and talk, PowerPoint Presentation

UNIT II

Quantum Algorithms: Key Quantum Algorithms and Their Relevance: Deutsch-Jozsa Algorithm for Testing Quantum Speedup, Grover's Algorithm for Quantum Search, Shor's Algorithm for Factoring and Cryptography. Quantum Fourier Transform (QFT), Simon's algorithm.

- Pedagogy/Course delivery tools: Chalk and talk, PowerPoint Presentation

UNIT III

Quantum Error Correction and Cryptography: Types of quantum errors and noise, Shor and Steane error-correcting codes, BB84 protocol and quantum key distribution, Security advantages of quantum cryptography.

- Pedagogy/Course delivery tools: Chalk and talk, PowerPoint Presentation

UNIT IV

Quantum Information Theory and Applications: Von Neumann entropy, Fidelity and quantum mutual information, Quantum teleportation and dense coding, Real-world applications.

- Pedagogy/Course delivery tools: Chalk and talk, PowerPoint Presentation

UNIT V

Programming a quantum computer: The IBM Qiskit/Qniverse/Cirq, Coding a quantum computer using a simulator to carry out basic quantum measurement and state analysis.

- Pedagogy/Course delivery tools: Chalk and talk, PowerPoint Presentation, IBM Qiskit/Qniverse/Cirq tools

Text Books:

1. Quantum Computation and Quantum Information, M. A. Nielsen &I.Chuang, Cambridge University Press (2013).
2. Quantum Computing: A beginners Introduction, Parag K. Lala, McGraw Hill; First Edition, 2020.

References:

1. Chris Bernhardt, Quantum Computing for Everyone, The MIT Press, Cambridge, 2020.
2. Phillip Kaye, Raymond Laflamme et. al., An introduction to Quantum Computing, Oxford

University press, 2007.
3. David McMahon-Quantum Computing Explained-Wiley-Interscience , IEEE Computer Society (2008).
4. Quantum Computing, A Gentle Introduction , Eleanor G. Rieffel and Wolfgang H. Polak MIT press(2014)

Course Outcome:

At the end of the course student will be able to:

1. Construct and analyze quantum circuits using basic and composite quantum gates. (PO-1,2,3,6,7; PSO:1,2)
2. Analyze Entanglement and Quantum Algorithms (PO-1,2, PSO-1,2)
3. Evaluate Quantum Error Correction and Cryptography Techniques (PO-3,4,5,PSO- 2,3)
4. Explore Quantum Information Theory and Applications (PO-5,9,10, PSO-1,2,3)
5. Design, implement, and analyze basic quantum programs using IBM Quantum Experience (IBMQiskit) or Qniverse and quantum simulators, including measurement and quantum state analysis.(PO-1,24,5-PSO-1,2)

Course Assessment and Evaluation:

Continuous Internal Evaluation (CIE): 50 Marks		
Assessment Tools	**Marks**	**Course Outcomes (COs) addressed**
Internal Test-I (CIE-I)	30	CO1, CO2
Internal Test-II CIE-II)	30	CO3, CO4, CO5
Average of the two CIE shall be taken for 30 marks		
Other Components		
Case study	10	CO1, CO2, CO3
Assignment/Quiz	10	CO4, CO5
The Final CIE out of 50 Marks = Average of two CIE tests for 30 Marks+ Marks scored in Case Study +Marks scored in Assignment		
Semester End Examination (SEE)	50	CO1, CO2, CO3 CO4, CO5

INSTITUTIONAL OPEN ELECTIVE – 1	
Course Code: CIOE0x*	**Credits: 3:0:0**
Prerequisite: Nil	**Contact Hours: 42L**
Course Coordinator: -	

Institutional Open Elective Courses:

Students belonging to a particular stream of Engineering and Technology are not entitled for the open electives offered by their parent department. However, they can take an elective offered by other departments, provided they satisfy the prerequisite condition, if any. Registration to open electives shall be documented under the guidance of the Program Coordinator/ Advisor/Mentor.

Selection of an open elective shall not be allowed if,

1. The candidate has studied the same course during the previous semesters of the program.
2. The syllabus content of open electives is similar to that of the Departmental core courses or professional electives.
3. A similar course, under any category, is prescribed in the higher semesters of the program.
4. The minimum students‘ strength for offering open electives is 10. However, this condition shall not be applicable to cases where the admission to the program is less than 10.

MINI PROJECT	
Course Code: CYP67	**Credits: 0:0:4**
Prerequisite: Nil	**Contact Hours: -**
Course Coordinator: Internal Guide	

Course Contents

Guidelines:
In order to address challenges within the realm of cutting-edge technologies, students are required to collaborate in groups of three or four. Each group focuses on solving a problem within a specific domain. To provide guidance and oversight of project advancement, an Internal Guide is assigned to each batch. These guides possess expertise in the relevant domain. Should the need arise, the Internal Guide is capable of organizing clarification sessions to address any uncertainties raised by the students working on the project. These interactions are duly documented for future reference.

Relevance of Project: Students are expected to articulate the significance of their project within the current IT landscape and broader society.
Literature Survey: Students must conduct a thorough review of research articles and existing projects to pinpoint gaps within the identified problem statement.
Design: Students are required to formulate a comprehensive design document encompassing class, use case, component diagrams, state models, sequence models, activity diagrams, and interaction models.
Implementation: Students should execute the designed model using appropriate techniques.
Presentation: Regularly, students are to present their progress to the evaluation committee. The committee evaluates based on the quality of the presentation, depth of content coverage, adeptness in addressing raised questions, and the evident division of teamwork. Scores are determined within this criterion for individual students.
Report and Publication: Each group must compose a project report and submit it to the department. Reports are expected to adhere to the standardized format set by the department. Each group must publish a paper in Scopus indexed conferences / journals as part of mini project.

Course Outcomes (COs):

At the end of the course Students will be able to:

1. Identify a problem, review research literature and analyse requirements (PO 1,12 PSO 1, 2, 3)
2. Schedule milestone and deliverables using appropriate project management techniques (PO 8,9,10,11 PSO 1,2, 3)
3. Design and implement the solution to selected problem using standard models and processes (PO 1,2,3,4,5,6,7,8,9, 10,11,12 PSO 1,2, 3)
4. Analyze the results and produce substantial written documentation (PO 1,2,4,8,9,10,11,12 PSO 1,2, 3)