PONDICHERRY UNIVERSITY
(A CENTRAL UNIVERSITY)

B.Sc. Cyber and Digital Sciences (Honors)

B.Sc. Cyber and Digital Sciences (Honors with Research)

REGULATIONS, CURRICULUM & SYLLABUS
(For Affiliated Colleges)

(Under the National Education Policy - NEP 2020)
Effective from the Academic Year (2023 - 2024)

Revised in June 2024

Board of Studies (BOS) - Computer Science

S.No.	Name	Affiliation	BoS
1	Dr. S.K.V. Jayakumar	Dept. of CS, Pondicherry University	Chairman
2	Dr. M. Punithavalli	Dept. of CA, Bharathiar University	External Members
3	Dr. P.S. Grover	Dept. of CS, Delhi University	
4	Dr. M. Sornam	Dept. of CS, University of Madras	Special Invitee
5	Dr. R. Subramanian	Dept. of CS, Pondicherry University	Members of Board
6	Dr. T. Chithralekha	Dept. of CS, Pondicherry University	
7	Dr. S. Bhuvaneswari	Dept. of CS, Pondicherry University	
8	Dr. R. Sunitha	Dept. of CS, Pondicherry University	
9	The Head, Dept. of CS	Dept. of CS, Achariya Arts & Sci. College	
10	The Head, Dept. of CS	Dept. of CS, Idhaya College of Arts & Sci.	
11	The Head, Dept. of CS	Dept. of CS, Avvaiyar Govt. College	
12	The Head, Dept. of CS	Dept. of CS, Don Bosco College	
13	The Head, Dept. of CS	Dept. of CS, PSV College of Arts & Sci.	
14	The Head, Dept. of CS	Dept. of CS, Rajiv Gandhi Arts & Science	

NEP Committee

S.No.	Name	Designation	Affiliation
1	Prof. S. K.V. Jayakumar	Professor and Head	Dept. of Computer Science, Pondicherry University
2	Prof. T. Chithralekha	Professor	
3	Prof. P. Sujatha	Professor	
4	Dr. R. Sunitha	Associate Professor	
5	Dr. V. Uma	Associate Professor	
6	Dr. K. S. Kuppusamy	Associate Professor	
7	Dr. M. Sathya	Assistant Professor	

Syllabus Revision Committee (Cyber and Digital Sciences)

S.No.	Name	Designation	Affiliation
1	Prof. T. Chithralekha	Professor	Dept. of Computer Science, Pondicherry University
2	Prof. P. Sujatha	Professor	
3	Dr. G. Krishnapriya	Assistant Professor	

Table of Contents

1. PREAMBLE & PROGRAMME OUTCOMES

1.1. Preamble

B.Sc. Cyber & Digital Science is an exceptional undergraduate degree program that caters to the ever-increasing demand for cybersecurity experts in today's digital era. This specialized course aims to provide students with a comprehensive understanding of the complex world of Cybersecurity and its application in safeguarding digital assets and information systems. As technology continues to advance, the demand for Cybersecurity professionals is soaring, making this degree program an attractive choice for individuals passionate about combating cyber threats and making a meaningful impact in the digital age. The course highlights a well-structured curriculum designed to equip students with in-depth knowledge and practical skills to address the complex challenges of Cybersecurity and digital technologies. The main objectives of the course are to:

- Develop technical proficiency in Cybersecurity, covering areas such as Network Essentials, Open Source Intelligence, Network Traffic Analysis, Ethical Hacking, Fundamentals of Cryptography, Cyber Law, and more.
- Nurture critical thinking, problem-solving, and innovation to empower the graduates to adapt and thrive in the ever-changing Cybersecurity industry.
- Introduce students to the niche areas of Cybersecurity and keep them abreast of the developments in the Cybersecurity industry.
- Prepare students for successful careers in Cybersecurity by offering practical hands-on experiences and opportunities for professional growth.
- Cultivate an interest for lifelong learning to ensure that our graduates remain at the forefront of technological advancements throughout their careers.
- Enable holistic, multidisciplinary, and skill-oriented knowledge development in the students.

Upon completing the programme, student can expect a plethora of promising career prospects and job opportunities in the cybersecurity domain. The cybersecurity industry is witnessing rapid growth and offers diverse roles across various sectors, making it an attractive field for aspiring professionals. Some of the prominent career paths and job opportunities for B. Sc. Cyber and Digital Science graduates include:

- Cybersecurity Analyst
- Information Security Officer

- Network Security Engineer
- Ethical Hacker
- Digital Forensics Analyst
- Cybersecurity Consultant
- Cloud Security Specialist
- Etc.

1.2. PROGRAMME OUTCOMES:

Upon completion of the Bachelor of Science (B.Sc.) programme in Cyber and Digital Sciences, students will demonstrate the following outcomes:

UG Certificate Level

• Attain foundational knowledge in Computer Networks and Cybersecurity.

• Ability to provide basic security for systems and networks.

UG Diploma Level

• Develop intermediate-level understanding and skills in Cybersecurity.

• Acquire hands-on skills to verify the Cybersecurity strength of computer systems and networks.

UG Degree Level

• Achieve advanced knowledge and proficiency in diverse areas of Cybersecurity.

• Demonstrate expertise in configuring and managing Cybersecurity for an organization's IT infrastructure.

UG Degree with Honors / Honors with Research

- Understand the fundamentals of Cybersecurity.
- Becoming conversant with the conventional and modern Cybersecurity technologies.
- Comprehend the various Cybersecurity attacks.
- Learn to compute the Cybersecurity risks faced by an organization.
- Ability to apply the technical and legal Cybersecurity expertise to manage the security of the IT infrastructure of an organization as per industry standards.
- Understand Artificial Intelligence and its uses for Cybersecurity management.

2. DEFINITIONS

Terms used in the NEP Regulations shall have the meaning assigned to them as given below unless the context otherwise requires:

A. Credit: A credit is the number of hours of instruction required per week for the given subject in a given semester of 16-18 weeks. One credit is equivalent to 15 hours of teaching (lecture or tutorial) or 30 hours of practice/field work/community engagement and service per Semester.

B. Academic Year: Means the year starting on 1st day of July and ends on the 30th day of June in the succeeding year.

C. Residence time: Means the time a student spends for attending classes in the College/Institution (either Online/Offline) as a full-time student and enrolled in any Academic programme of the Institution.

D. Semester: Means 18 weeks (90 Working days) of teaching-learning sessions of which two weeks shall be set apart for examinations and evaluation.

E. Grade: Means a letter grade assigned to a student in a Course for his/her performance at academic sessions as denoted in symbols of : O(Outstanding), A+(Excellent), A (Very good), B+ (Good), B (Above Average), C (average), P (Pass), F (Fail) and Ab (Absent) with a numeric value of O=10, A+=9, A=8, B+=7, B=6, C=5 P=4, and F=0, Ab=0.

F. Grade Point Average (GPA): Means an average of the Grades secured by a student in all courses in a given academic session duly weighted by the number of credits associated to each of the courses.

G. Cumulative GPA (CGPA): Means the weighted average of all courses the student has taken in a given Programme.

H. A Common Course: Means the set of courses that all students who are admitted to any Programme of the University are required to study these courses include, Languages (English-Modern Indian Languages), NEP specific courses- viz. Understanding India, Environmental sciences/Education, Health and Wellbeing/Yoga, Digital & Technological solutions.

I. Major Discipline: Means the core subjects mandatory for the programme, Major discipline may be a single discipline or interdisciplinary/ multidisciplinary courses. Eg. B.Sc. (Physics) or B.Sc. (Physics, Maths and Chemistry).

J. Minor Discipline: Means the courses which are specific to the specialization in Computer Science.

K. Credit Requirement: For a Degree/Diploma/Certificate Programme means the minimum number of credits that a student shall accumulate to achieve the status of being qualified to receive the said Degree, Diploma/Certificate as the case may be.

L. Exit option: Means the option exercised by the students, to leave the Programme at the end of any given Academic year.

M. Lateral entry: Means a student being admitted into an ongoing Programme of the University otherwise than in the 1st year of the programme.

N. Vocational Studies/Education: This refers to set of activities for participation in an approved project or practical or lab, practices of application of scientific theories, studio activities involving students in creative artistic activities, workshop-based activities, field-based shop-floor learning, and Community engagement services, etc. (These courses are expected to enable students to incorporate the learned skills in daily life and start up entrepreneurship.)

O. Skill-based learning/project: This refers to activities designed to understand the different socio-economic contexts, first-hand understanding of the policies, regulations, organizational structures, processes, and programmes that guide the development process.

P. Work-based internship: Means structured internships with Software Companies, Research and Higher Educational Institution Laboratories, Corporate offices, etc. which will further improve employability.

3. DURATION, ELIGIBILITY & AWARD OF UG DEGREE / DIPLOMA / CERTIFICATE

3.1. Duration of the Programme

The duration of the UG programme is 4 years or 8 semesters. Students who desire to undergo a Three-year UG Programme will be allowed to exit after completion of the 3rd year. If a student wants to leave after the completion of the first or second year, the student will be given a UG Certificate or UG Diploma, respectively, provided they secure the prescribed number of credits (as given in Table 1).

3.2. Eligibility

Senior Secondary School Leaving Certificate or Higher Secondary (12th Grade) Certificate obtained after successful completion of Grade 12 or equivalent stage of education corresponding to Level-4 (Levels in NHEQF). **For detailed eligibility, refer the Admissions and Lateral Entry Section 5.**

3.3. Awarding of UG Certificate, UG Diploma and Degrees Nomenclature

Four years B.Sc. Degree Programme shall have options for earning a Certificate / Diploma / UG Degree / UG Degree (Honors) / UG Degree (Honors with Research) based on the exit option exercised by the candidates.

3.3.1. UG Certificate

Students who opt to exit after completion of the first year (2 Semesters) and have earned a minimum of 40 credits will be awarded a Certificate in Cybersecurity if, in addition, they complete work based vocational courses / internship of 4 credits during the summer vacation of the first year.

3.3.2. UG Diploma

Students who opt to exit after completion of the second year (4 Semesters) and have earned a minimum of 80 credits will be awarded the UG diploma in Cyber and Digital Sciences if, in addition, they complete work based vocational courses / internship of 4 credits during the summer vacation of the second year.

3.3.3. Three-year UG Degree

Students who wish to discontinue after the 3-year (6 Semesters) UG programme will be awarded a UG Degree in Cyber and Digital Sciences after successful completion of three years, earning a minimum of 120 credits and satisfying the minimum credit requirements as mentioned in Table 1.

3.3.4. Four-year UG Degree (Honors)

A four-year UG Honors degree in Cyber and Digital Sciences will be awarded to those who complete a four-year (8 Semesters) degree programme, earning a minimum of 160 credits and have satisfied the credit requirements as mentioned in Table1.

3.3.5. Four-year UG Degree (Honors with Research)

Students who secure a minimum of 7.5 CGPA in the first six semesters and wish to undertake research at the undergraduate level can choose a research stream in the fourth year. They should do a research project or dissertation under the guidance of a faculty member of the University.

The research project/dissertation will be in the major discipline, Cyber and Digital Sciences. The students who secure a minimum of 160 credits, including 12 credits from a research project/dissertation, will be awarded UG Degree in Cyber and Digital Sciences (Honors with Research).

3.3.6. Programme overview

As per the guidelines of NEP, students are mandated to complete 120 credits to complete a basic Bachelor's Degree in 3 years. With an additional 40 credits of course work one can pursue 4^{th} Year Honors or Honors with Research Degree. The UG Programme will consist of the following categories of courses and the minimum credit requirements for 3-year UG and 4-year UG(Honors) or UG (Honors with Research) programmes are given in Table 1.

Table 1: Breakup of Credits and Courses – Minimum Requirements

S.No.	Component	3 Year UG	4 Year UG (Honors/ Honors with research)
1	Major Disciplinary - Computer Science	60 Credits (15 Courses of 4 credits)	80 Credits (20 Courses of 4 credits)
2	Minor Disciplinary – Specialization Courses	24 Credits (6 Courses of 4 Credits)	32 Credits (8 Courses of 4 credits)
3	Multi-Disciplinary Courses	9 Credits (3 courses of 3 credits)	9 Credits (3 courses of 3 credits)
4	Ability Enhancement Courses	8 Credits (4 courses of 2 credits)	8 Credits (4 courses of 2 credits)
5	Skill Enhancement Course – On the chosen Specialization	9 Credits (3 courses of 3 credits)	9 Credits (3courses of 3 credits)
6	Value-added courses	8 Credits (4 courses of 2 credits)	8 Credits (4 courses of 2 credits)
7	Summer internship	4 Credits (Included in Major courses of 60 credits)	4 Credits (Included in Major courses of 80 credits)
8	Community engagement and service	2 Credits (1 Field based Course)	2 Credits (1 Field based Course)
9	Research Dissertation Project	-	12 Credits
	Total	**120**	**160**

Note: Honors students not undertaking research will do 3 courses for 12 credits in lieu of a Research Project / Dissertation.

3.3.7. Degree and Nomenclature

Candidates who complete Eight semesters and earn a minimum of 160 credits and have satisfied the credit requirements as mentioned in the Table 1 will be awarded either of the following degrees.

- B.Sc. Cyber and Digital Sciences *
- B.Sc. Cyber and Digital Sciences (Honors) #
- B.Sc. Cyber and Digital Sciences (Honors with Research)##

* for candidates who wish to exit at the end of third year with 120 credits earned and satisfied the other minimum requirements given in 3.3.9.

for candidates who complete 3 theory courses (MJD 21, MJD 22, and MJD 23) instead of the research project work in the Eighth Semester.

for candidates who complete a research project work in the Eighth Semester.

3.3.8. Degree with Specialization

Out of the above said 160 credits (Table1) the candidates shall earn 103 credits (83 credits out of 120 credits in the case of 3 year UG) from the Hardcore courses (Major Disciplinary, Multi-disciplinary, Ability Enhancement, Value added Courses and Community Engagement and Service) and the remaining 57 credits (37 credits in the case of 3 year UG) shall be earned from the subjects they choose to study from the list of softcore courses. These 57 credits shall be earned through studying the specialization courses in Minor Disciplinary – Specialization Courses, Skill Enhancement Courses in all the semesters and the Research Project or the Courses the candidates choose to study in the Eighth Semester. The Programme Structure is detailed in the following Figure 1.

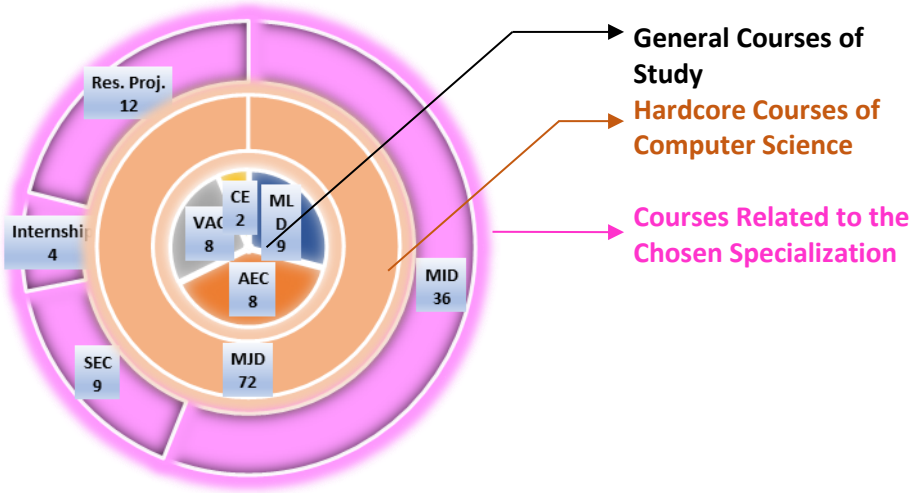

Figure 1: Programme Structure with credit breakup

3.3.9. Exit Options and Nomenclature of Certificate, Diploma

Candidates can exercise the following exit options and obtain the said certificate or diploma or degree, if the minimum required credits are earned and other conditions are met. Students exercising the option of exit at the end of 2nd semester or 4th semester need to have completed an internship for atleast 8 weeks along with the necessary credit requirements to qualify for the relevant certificate or diploma. In any case, every student, whenever exit (or complete the 4

year programme), should have completed atleast one internship for a minimum period of 8 weeks.

Exit after 2nd Semester: Certificate in Cybersecurity will be awarded for candidates who exit the course at the end of 2nd semester and earned a minimum of 40 credits and have completed a Summer Internship of 4 credits for a minimum period of 8 weeks, during the summer vacation post 2nd semester.

Exit after 4th Semester: Diploma in Cyber and Digital Sciences will be awarded for candidates who exit the course at the end of 4th semester and earned a minimum of 80 credits and have completed a Summer Internship of 4 credits for a minimum period of 8 weeks, during the summer vacation post 4th semester.

Exit after 6th Semester: UG Degree in Cyber and Digital Sciences (B.Sc. (CDS)) will be awarded for candidates who exit the course at the end of 6th semester and earned a minimum of 120 credits and have completed a Summer Internship of 4 credits for a minimum period of 8 weeks, during the summer vacation post 4th semester.

Exit after	Credits and other requirements	Awards
2nd Semester	Min: 40 Credits & Internship	Certificate in Cybersecurity
4th Semester	Min: 80 Credits & Internship	Diploma in Cyber and Digital Sciences
6th Semester	Min: 120 Credits & Internship	B.Sc. Cyber and Digital Sciences

4. STRUCTURE OF THE UNDERGRADUATE PROGRAMME

This B.Sc Honors programme offered in the affiliated colleges shall confirm to the structure specified hereunder. As per the decided programme mandate, the students to complete 120 credits to complete a basic Bachelor's Degree in 3 years. With an additional 40 credits of course work one can pursue 4th Year Honors or Honors with Research Degree. The UG Programme will consist of the categories of courses and the minimum credit requirements for 3-year UG and 4-year UG(Honors) or UG (Honors with Research) programmes as given in Table 1 at Section 3.3.6.

4.1. Types of Courses

Hardcore Courses	Softcore Courses (Specialization specific)
Major Disciplinary–Cyber and Digital Sciences	Minor Disciplinary
Multi-Disciplinary Courses	Skill Enhancement Courses
Ability Enhancement Courses	Summer Internship
Value Added Courses	Research Dissertation Project
Community Engagement and Service	

4.2. Description of Courses

The following are the types of courses in this programme:

4.2.1. Major Discipline: 60 Credits - 3 Year UG, & 72 Credits - 4 Year UG

Major discipline (Cyber and Digital Sciences) : Students should secure the prescribed number of credits (not less than 50% of the total credits) through core courses in the major discipline. The major discipline would provide the opportunity for a student to pursue in-depth study of a particular subject or discipline. A student may choose to change the major discipline within the broad discipline at the end of the second semester provided all the prerequisites of the respective degree programme are fulfilled.

4.2.2. Minor Discipline / Specialization: 24 Credits - 3 Year UG & 40 Credits - 4 Year UG

Minor discipline helps a student to gain a broader understanding beyond the major discipline.

4.2.3. Multidisciplinary courses (MD): 9 Credits

All undergraduate students are mandated to pursue 9 credits worth of courses in such multi-disciplinary areas / Courses out of 9/10 NEP defined subjects. Colleges may identify any 3 multiple disciplinary streams listed below based on availability of resources and manpower.

a) Natural Sciences
b) Physical Sciences
c) Mathematics & Statistics
d) Computer Science/Applications
e) Data Analysis
f) Social Sciences
g) Humanities
h) Commerce & Management
i) Library Science
j) Media Sciences, etc.

Students are expected to learn basic/introductory courses designed by other departments for this purpose. Colleges may list any 3 introductory courses (one each in Natural Sciences, Physical Sciences & Humanities) for uniform adoption of all UG students.

4.2.4. Ability Enhancement Courses (AEC): 8 credits

All Undergraduate (UG) students are mandated to complete at least 8 Credits worth of Courses which focus on Communication and Linguistic skills, Critical reading and Writing skills. These courses are expected to enhance the ability in articulation and presentation of their thoughts at workplace. Colleges may design these ability enhancement courses tuned to the requirements of given major discipline. For example, a course in Business Communication is more appropriate in place of literature/prose/poetry.

Ability Enhancement Course	
I. English Language	**II. Indian Language (two courses)**
a. English Language & Literature - 1 and 2	a. Indian language & Literature - 1 and 2
b. Functional English - 1 and 2	b. Functional language - 1 and 2
c. Communicative English - 1 and 2	c. Communicative language - 1 and 2

4.2.5. Skill Enhancement Courses (SEC): 9 credits

These courses are aimed at imparting practical skills, hands-on training, soft skills, and other skills to enhance the employability of students. Courses are designed as per the students' needs with the available resources. Students can choose these courses from the list of courses offered in the chosen specialization as said in 4.2.2. Colleges may also outsource the Skill Enhancement Courses to AICTE approved agencies for conducting short term Training Workshops, Skill India initiatives of GOI and approved Trades by Skill development of corporation are to be considered.

4.2.6. Value-Added Courses (VAC) Common to All UG Students: 8 credits

Under NEP, the UGC has proposed for 6 to 8 credits worth of common courses which are likely to add value to overall knowledge base of the students. These courses include:

a) Understanding India

b) Environmental Sciences/Education/Higher Order Thinking

c) Digital and Technological solutions

d) Health, Wellness, Yoga Education, Sports & Fitness/Universal Human Values

The course structure and coverage of topics are suggested by UGC in its draft documents, colleges/UG Boards of Studies may design the methodology for conducting these value added courses.

4.2.7. Summer Internship: 4 Credits

All students will undergo Internships / Apprenticeships in a firm, industry, or organization or Training in labs with faculty and researchers in their own or other Higher Education Institutions / Research institutions during the summer term. Students will be provided with opportunities for internships to actively engage with the practical side of their learning. Such Summer Internship is to be conducted in between 4th Semester and 5th Semester. A review report and award of grade based on Work based learning by students is to be recorded during the 5th Semester. Students who exercise the option of exit at the end of 1st year or 2nd year need to do the internships as specified in the respective section.

4.2.8. Community Engagement and Service: 2 Credits

The curricular component of 'Community Engagement and Service' seeks to expose students to the socio-economic issues in society so that the theoretical learnings can be supplemented by actual life experiences to generate solutions to real-life problems. This can be part of summer term activity or part of a major or minor course. Community Engagement shall be conducted for a minimum of 2 weeks.

4.2.9. Research Project / Dissertation: 12 Credits

Students choosing a 4 Year Bachelor's degree (Honors with Research) are required to take up research projects under the guidance of a faculty member. The students are expected to complete the Research Project in the eighth semester.

4.2.10. Audit courses: 0 credits

Audit courses offered do not carry any credits. Evaluation will be based on continuous assessment. Students may be given a Pass or Fail (P/F) based on the assessment that may consist of class tests, homework assignments, and/or any other innovative assessment methodology suitable to the expected learning outcome, as determined by the faculty in charge of the course of study.

4.3. Levels of the Courses

Course codes are based on the academic rigor. The first four letters of the course code indicate the department/Centre, followed by the academic rigor level code in digits. The coding structure follows:

4.3.1. 0-99: Pre-requisite courses

It is required to undertake an introductory course which will be a pass or fail course with no credits. It will replace the existing informal way of offering bridge courses that are conducted in some of the colleges/ universities.

4.3.2. 100-199: Foundation or introductory courses

These are courses which are intended for students to gain an understanding and basic knowledge about the subjects and help decide the subject or discipline of interest. These courses generally would focus on foundational theories, concepts, perspectives, principles, methods, and procedures of critical thinking in order to provide a broad basis for taking up more advanced courses.

4.3.3. 200-299: Intermediate-level courses including subject-specific courses

These courses are intended to meet the credit requirements for minor or major areas of learning. These courses can be part of a major and can be pre-requisite courses for advanced-level major courses.

4.3.4. 300-399: Higher-level Courses

These courses are required for majoring in a disciplinary/interdisciplinary area of study for the award of a degree.

4.3.5. 400-499: Advanced Courses

These courses which would include lecture courses with practicum, seminar-based course, term papers, research methodology, advanced laboratory experiments/software training, research projects, hands-on-training, internship/apprenticeship projects at the undergraduate level or first year post-graduate theoretical and practical courses.

4.4. Credit-hours for different types of courses

A three-credit lecture course in a semester means three one-hour lectures per week with each one-hour lecture counted as one credit. One credit for tutorial work means one hour of engagement per week. A one-credit course in practicum or lab work, community engagement and services, and fieldwork in a semester mean two-hour engagement per week.

The Faculty to Student Ratio in all the practical / laboratory classes shall be maintained at 1:25.

In a semester of 15 weeks duration, a one-credit practicum in a course is equivalent to 30 hours of engagement. A one-credit of Seminar or Internship or Studio activities or Field practice/projects /community engagement and service means two-hour engagements per week. Accordingly, in a semester of 15 weeks duration, one credit in these courses is equivalent to 30 hours of engagement.

4.4.1. Pedagogical Styles

In order to achieve the expected Learning outcomes, UGC Framework has specified different Pedagogical approaches for different courses at undergraduate level. These approaches include:

a) Lecture course
b) Tutorial course
c) Practice cum or laboratory courses
d) Seminar Course
e) Internship course
f) Studio activity-based course
g) Field practicing
h) Project work courses
i) Community engagement and service course

The details of these different types of Pedagogical methods are as follows:

Table2: Pedagogical Approaches

COURSE TYPES	APPROACH
Lecture Courses	Regular classroom lectures by qualified / experienced Expert Teachers ● These Lectures may also include classroom discussion, demonstrations, case analysis ● Use of Models, Audio-Visual contents, Documentaries, PPTs may supplement.
Tutorial Courses	Problem solving Exercise classes guided discussion, supplementary readings vocational training, etc.
Practical / Lab work	Practical Lab activity with Theoretical support Mini projects, Activity based engagement, Program executions, Data processing and presentation exercise.
Seminar Course	A course requiring student to design and participate in discussions, Group Discussions, Elocution and Debate, Oral Communication Paper presentations, Poster Presentation, Role play participation, Quiz competitions, Business plan preparation/presentation, etc.
Internship course	Courses requiring students to *Learn by Doing* in the workplace external to the educational Institutions. Internships involve working in Software Companies, Research and Higher Educational Institution Laboratories, Corporate Offices, etc. All Internships should be properly guided and inducted for focused learning.
Research Project	Students need to study and analyze the recent research publications from indexed/peer reviewed journals in their area of specialization. Outcome of the study and analysis need to be presented as a thesis or research report with necessary experimental results.

4.5. Semester-wise Break: for courses of 3 year UG and 4 Year UG(Hons) Degree programmes

Incorporating the focus of NEP in terms of different categories of courses and award of Certificates, Diplomas and Degrees during different stages of 4 year Degree programmes, a template for Semester-wise course work was designed by the UGC and presented in para 5.3 of Curriculum Framework . Salient features of it are as follows:

- All courses shall carry specified number of credits.
- Every Semester shall have a minimum of 20 credits worth of courses.
- Credits for a course shall be decided on the basis of number of Contact hours of the teaching in a classroom.
- One credit means one hour of Teaching in the case of a Theory subject and at least 2 hours of conducting Practical in the case of Lab subjects.

- All Major and Minor disciplinary Courses shall have 4 credits with 6 hours of work load (including 2 hours of tutorials)

- Language courses, ability enhancement, skill enhancement and value added common course also will have 2 hours of hands on training.

- Progress of Learning is measured in terms of credits earned by the students on successful completion of the course.

- Students can exercise his/her choice for exiting the course at the end of every Academic year.

- Graduate attributes listed by UGC shall be the focus of Teaching-Learning process.

- Semester I and II shall focus on introductory courses/subjects in Major/Minor disciplines and shall focus on providing knowledge in Multidisciplinary areas, skill enhancement and ability enhancement courses.

- Semester III and IV shall focus on Core disciplinary courses with a focus on building strong foundation in the given Discipline.

- Semester V and VI shall focus on providing in-depth knowledge and skills required for taking up a career in the given discipline.

- Semester VII and VIII shall focus on Advanced knowledge and shall direct the students to take up socially relevant projects/Research works newer applications of the knowledge.

5. ADMISSION ELIGIBILITY, LATERAL ENTRY

5.1 Admission Eligibility

The candidates for admission to this programme shall be required to have passed 10+2 / 10+3 system of examinations or equivalent with Mathematics / Business Mathematics / Computer Science / Computer Applications / Informatics Practices / or Equivalent as one of the subjects of study.

Students shall be admitted to this programme based on admissions criteria fixed by the University / Government of Puducherry from time to time.

5.2 Admissions by Lateral Entry

In this programme, where admission was carried out adopting approved procedures in preceding years, subject to availability, lateral entry admission shall be permitted, subject to:

Candidates seeking entry at the second, third and fourth year, should meet the necessary eligibility criteria with respect to the certificate / diploma / degree they possess, with necessary minimum credits banked in the Academic Bank of Credits (ABC). Such students who get admitted in later years, other than first year will be guided by the following clauses:

- That the University shall notify the admission process and number of vacancies open for lateral entry.
- That the Lateral entrants shall be admitted only after such transparent screening process and such procedure that the University may prescribe from time to time. University may prescribe different methods of screening for different programmes depending on the circumstances prevailing in each case.
- Lateral entry shall be permissible only in the beginning of years 2, 3, 4 of the Under Graduate / Honors programme; provided that the students seeking lateral entry shall have obtained the minimum pass marks / grades fixed by the University in their previous academic years.

6. EVALUATION

All Credit courses are evaluated for 100 marks. Internal Assessment component is for 25 marks and the End Semester University exam is for 75 marks. In case of Practicals, Project work etc., it is 50 marks for Internal and 50 marks for End-Semester Exams.

6.1. Category of Courses

There are three category of courses as shown in 6.2. Category A, theory courses with lecture hours and tutorials are evaluated for an Internal assessment component of 25 Marks and End Semester University Exam for 75 Marks.

Category A	Theory Courses with Lecture hours and hours allotted for Tutorials wherever required.
Category B	Practical Courses with only Practical hours or Laboratory hours. Laboratory Courses, Internships, Research Project Works and other courses allotted only with practical hours in the curriculum shall be under this category.
Category C	Theory & Practice combined Courses where Lecture and Practical hours allotted.

6.2. Learning Assessment

<table>
<tr><th>Course Types</th><th>Internal Assessment</th><th>End Semester Assessment</th></tr>
<tr><td>Category A

IA: 25 Marks
EA: 75 Marks</td><td>25 Marks
<table><tr><th>Evaluation Component</th><th>Marks</th></tr><tr><td>I. Mid Semester Exam (one)</td><td>20</td></tr><tr><td>II. Percentage of Attendance</td><td>05</td></tr><tr><td>Total</td><td>25</td></tr></table></td><td>75 Marks

(Evaluation Details given in Table 3)</td></tr>
<tr><td>Category B

IA: 50 Marks
EA: 50 Marks</td><td>50 Marks
For Practical / Internship Courses<table><tr><th>Evaluation Component</th><th>Marks</th></tr><tr><td>I. Weekly Observation Book / Report</td><td>15</td></tr><tr><td>II. Practical Record / Internship Report</td><td>15</td></tr><tr><td>III. Model Practical Exam</td><td>15</td></tr><tr><td>IV. Percentage of Attendance</td><td>05</td></tr><tr><td>Total</td><td>50</td></tr></table>For Research Project Work Course<table><tr><th>Evaluation Component</th><th>Marks</th></tr><tr><td>I. Monthly Review (3 Reviews – 10 Marks each)</td><td>30</td></tr><tr><td>II. Project Report</td><td>10</td></tr><tr><td>III. Project Work</td><td>10</td></tr><tr><td>Total</td><td>50</td></tr></table></td><td>50 Marks

(Evaluation Details given in Table 3)</td></tr>
<tr><td>Category C

IA: 25 Marks
EA: 75 Marks</td><td>25 Marks
<table><tr><th>Evaluation Component</th><th>Marks</th></tr><tr><td>I. Mid Semester Exam (one) - Theory</td><td>10</td></tr><tr><td>II. Observation Book, Record Book</td><td>10</td></tr><tr><td>III. Percentage of Attendance</td><td>05</td></tr><tr><td>Total</td><td>25</td></tr></table></td><td>75 Marks

(Evaluation Details given in Table 3)</td></tr>
</table>

6.3. Marks for Attendance

Attendance %	Marks
Below 75%	0
75% - 80%	1
81% - 85%	2
86% - 90%	3
91% - 95%	4
96% - 100%	5

6.4. Internal Test Scheme

Principal of the College schedules the Mid-Semester Exam for all courses during 8/9th week of start of classes. All faculty members are expected to conduct this Mid-Semester exam for 1½ hour duration and evaluate, upload the marks to Controller of Examinations of University. Colleges need to preserve the answer books of Mid-Semester exams until declaration of results by the University.

6.5. End Semester University Exam

Controller of Examinations (COE) of Pondicherry University schedules the End-Semester exams for all three categories of courses. **For Category C courses, theory and practical exams will be conducted separately by the Controller of Examinations of Pondicherry University.**

A detailed Exam Time Table shall be circulated to all Colleges atleast 15 days before the start of exams mostly during 15/16th week of the Semester. Question Papers shall be set externally based on BOS approved syllabus. All students who have a minimum of 70% attendance are eligible to attend the end-semester exams. The breakup of end semester marks is as given below.

6.6. Break up of end semester marks
(All End Semester Exams shall be conducted by the Pondicherry University)

The question paper shall be set as per the Bloom's Taxonomy. Table3 below gives the details of evaluation methods for Category A, B and C courses. Various levels along with their description and sample questions are as follows:

Knowledge: Recall or remember previously learned information.

Example: List the basic data types in Python

Comprehension: Demonstrate understanding of facts and ideas by organizing, comparing, translating, interpreting, giving descriptions, and stating the main ideas.

Example: Explain how a stack data structure works.

Application: Apply knowledge and concepts to solve problems in new situations. Use learned information in a different context.

Example: Write a Python program to solve the deadlock problem.

Analysis: Break down information into parts and examine the relationships between the parts. Identify motives or causes.

Example: Analyse the efficiency of two sorting algorithms and compare their advantages and disadvantages.

Synthesis: Create a new whole by combining elements in novel ways. Use creativity to produce something original.

Example: Design a web application that can generate a time table of a school.

Table3: End Semester Assessment examination details for all three categories of courses

Course Components	Marks	Duration
Category A. Theory subjects: Sec A: 10 Questions of 2 Marks each (20 Marks) *(Knowledge: 3, Comprehension: 2, Application: 3, Analysis:2)* Sec B: 5 out of 7 Questions of 5 Marks each (25 Marks) *(Knowledge: 1, Comprehension: 2, Application: 1, Analysis:3)* Sec C: 2 Either/OR choice questions of 15 Marks each (30 Marks) *(Application: 2 Analysis:2* **Questions from all units of Syllabus equally distributed.**	75 Marks	3 Hours
Category B. Skill Enhancement / Practical Courses Based on Practical Exams conducted by COE of University **Internship / Research Project Work:** Presentation of the work / Report / Viva-voce examinations conducted by COE of university.	50 Marks	3 Hours --
Category C. Theory Subjects with Practical Components: **i. Theory Component:** Sec A: 5 Questions of 2 Marks each (10 Marks) *(Knowledge: 3, Comprehension: 2, Application: 3, Analysis:2)* Sec B: 5 out of 7 Questions of 4 Marks each (20 Marks) *(Comprehension: 2, Application: 3, Analysis:2)* Sec C: 2 Either or type questions of 10 Marks each (20 Marks) *(Analysis / Synthesis)* **Questions from all units of Syllabus equally distributed.** **ii. Practical Component:** Based on Practical Exams conducted by COE of University **The examination shall be conducted for 50 Marks and reduced to 25 Marks.** **Total Marks: 75 (Theory: 50 Marks + Practical: 25 Marks)**	50 Marks 25 Marks	3 Hours 3 Hours

7. CONSOLIDATION OF MARKS, PASSING MINIMUM AND ARREAR EXAM

Controller of Examinations of the University consolidates the Internal Assessment marks uploaded by the Colleges and marks secured by students in end-semester examination. The total marks will be converted into letter grades as shown in the table Section 8.1.

7.1. Passing Minimum

As per NEP Regulations, the passing minimum is 50% marks (IA + End semester put together). However, Pondicherry University considers 40% marks as pass during first 3 years of study and students who secured less than 50 will be awarded 'P' (Pass Grade).

7.2. Arrear Exam

A student who failed to secure 50% marks in aggregate is declared as Failed. Failed students are eligible to take up supplementary examination by registering to the failed course in the following Semester. All other candidates who failed due to shortage of attendance, those who are seeking to improve the grade shall repeat the course.

8. LETTER GRADES AND RANGE OF MARKS

Total Marks secured by a student in each subject shall be converted into a letter grade. UGC Framework has suggested a Country wide uniform letter grades for all UG courses.

8.1. Letter Grades

The following Table shows the seven letter grades and corresponding meaning and the grade points for calculation of CGPA.

Letter Grade	Grade Point
O (outstanding)	10
A+ (Excellent)	9
A (Very good)	8
B+ (Good)	7
B (Above average)	6
C (Average)	5
P (Pass)	4
F (Fail)	0
Ab (Absent)	0

In order to work out the above letter grades, the marks secured by a student (Total of Internal Assessment and End Semester Assessment) would be categorized for relative grading.

8.2. Range of Marks for each letter grades

The ranges of marks for each grade would be worked as follows:

Highest marks in the given subject	X
Cut of marks for grading purpose	50 Marks
Passing mark (for 3 year UG)	40 Marks
Number of grades G (Excl. P grade)	Grades: O, A+, A, B+, B, C, Hence, **G = 6**
Range of marks	K
K = (X – 50) / G	

The following table gives the range of marks and letter grades. According to K value, one of the following grading scheme will be followed.

(i) If $K \geq 5$, then the grades shall be awarded as given in the following table.

Range of Marks in %	Letter Grade Points for	Grade Points for
X to (X-K) + 1	O	10
(X-K) to (X-2K) + 1	A+	9
(X-2K) to (X-3K) + 1	A	8
(X-3K) to (X-4K) + 1	B+	7
(X-4K) to (X-5K) + 1	B	6
(X-5K) to 50	C	5
40 – 49	P	4
Below 40	F	0
Absent (Lack of Attendance)	Ab	0

(ii) If K< 5, then the grades shall be awarded as given in the following table.

Range of Marks in %	Letter Grade Points for	Grade Points for
80-100	O	10
71-79	A+	9
66-70	A	8
61-65	B+	7
56-60	B	6
50-55	C	5
40-49	P	4
Below 40	F	0
Absent (lack of attendance)	Ab	0

9. CALCULATION OF SGPA & CGPA

Semester Grade Point Average (SGPA) is calculated by taking a weighted average of all grade points secured by a candidate from all subjects registered by him/her in the given Semester. The weights being the number of credits that each subject carries.

Cumulative Grade Point Average (CGPA) shall be calculated as the weighted average of credits that course carries and the value of Grade points averaged for all subjects.

9.1. Procedure of computation of SGPA and CGPA

The following procedure shall be followed to compute the Semester Grade Point Average (SGPA) and Cumulative Grade Point Average (CGPA):

The SGPA is the ratio of the sum of the product of the number of credits with the grade points scored by a student in all the courses taken by a student and the sum of the number of credits of all the courses undergone by a student, i.e. $SGPA\ (Si) = \Sigma(Ci \times Gi) / \Sigma Ci$

Where Ci is the number of credits of the i^{th} course and Gi is the grade point scored by the student in the i^{th} course.

9.2. Example for Computation of SGPA where candidate has not failed in any course.

Semester	Course	Credit	Letter Grade	Grade Point	Credit Point (Credit x Grade)
I	Course 1	3	A	8	3 X 8 = 24
I	Course 2	4	B+	7	4 X 7 = 28
I	Course 3	3	B	6	3 X 6 = 18
I	Course 4	3	O	10	3 X 10 = 30
I	Course 5	3	C	5	3 X 5 = 15
I	Course 6	4	B	6	4 X 6 = 24
		20			139
	SGPA				139/20=6.95

9.3. Example for Computation of SGPA where candidate has failed in one course.

Semester	Course	Credit	Letter Grade	Grade Point	Credit Point (Credit x Grade)
I	Course 1	3	A	8	3 X 8 = 24
I	Course 2	4	B+	7	4 X 7 = 28
I	Course 3	3	B	6	3 X 6 = 18
I	Course 4	3	O	10	3 X 10 = 30
I	Course 5	3	C	5	3 X 5 = 15
I	Course 6	4	F	0	4 X 0 = 00
		20			115
	SGPA				115/20=5.75

9.4. Example for Computation of SGPA where candidate has failed in two courses.

Semester	Course	Credit	Letter Grade	Grade point	Credit Point (Credit x Grade)
I	Course 1	3	A	8	3 X 8 = 24
I	Course 2	4	B+	7	4 X 7 = 28
I	Course 3	3	F	0	3 X 0 = 00
I	Course 4	3	B	6	3 X 6 = 18
I	Course 5	3	C	5	3 X 5 = 15
I	Course 6	4	F	0	4 X 0 = 00
		20			85
	SGPA				85/20=4.25

The CGPA shall also be calculated in similar way as shown in examples (i), (ii) and (iii) of SGPA for all subjects taken by the students in all the semesters. However, if any student fails more than once in the same subject, then while calculating CGPA, the credit and grade point related to the subject in which the student fails in multiple attempts will be restricted to one time only. The SGPA and CGPA shall be rounded off to 2 decimal points and reported in the transcripts.

In case of audit courses offered, the students may be given (P) or (F) grade without any credits. This may be indicated in the mark sheet. Audit courses will not be considered towards the calculation of CGPA.

10. DECLARATION OF RESULTS

Controller of Examinations (COE) of the University shall declare the results of given UG programme following the CGPA secured by students by the end of 6th Semester and 8th Semester.

Pass Classes:

Range of CGPA	Result
9.0 - 10	First Class with distinction
6.0 - 8.99	First Class
5.0 - 5.99	Second Class
4.0 - 4.99	Pass Class

11. MINIMUM CREDIT REQUIREMENTS

S.No	Component	3-years UG			4-years UG (Honors / Honors With research)		
		Credits	Courses	Cr/Course	Credits	Courses	Cr/Course
1	Major Disciplinary/ Interdisciplinary Courses	56	14	4	76	19	4
2	Minor Disciplinary/ Interdisciplinary Courses	24	6	4	32	8	4
3	Multi-Disciplinary Courses	9	3	3	9	3	3
4	Ability Enhancement Courses	8	4	2	8	4	2
5	Skill Enhancement Courses	9	3	3	9	3	3
6	Value-added courses	8	4	2	8	4	2
7	Summer Internship (MJD 11)	4		4	4	1	4
8	Community Engagement and Service	2	1	2	2	1	2
9	Research Project/Dissertation	--	--	--	12	Project or 3 Courses##	
Total		**120**			**160**		

##Note: *Honors students not undertaking research will do 3 courses for 12 credits in lieu of a research project/Dissertation.*

- *MJD: Major Disciplinary (Compulsory – Hardcore Subjects)*
- *MID: Minor Disciplinary (Specialization Specific – Softcore Subjects)*
- *MLD: Multi-Disciplinary*
- *AEC: Ability Enhancement Courses*
- *SEC: Skill Enhancement Courses*
- *VAC: Value Added Courses*

12. COURSE CODE

- **Course code :** 7 Characters: 4 Alphabets and 3 Digits. Ex : ABCD123
- **Alphabets :** 1st and 2nd Alphabets: Major domain
  3rd and 4th Alphabets: Specialization
- **Digits :** 1st Digit: Levels (100, 200, 300, 400…)
  2nd and 3rd Digits: Serial number of the courses in the given year

Example: CSCY312: Computer Science Cyber and Digital Sciences, Level 300, Serial number of the course in the year (12).

B.Sc. CYBER AND DIGITAL SCIENCES

CURRICULUM

FIRST SEMESTER								
S. No	Component	Course Code	Title of the Course	H/S	Credits	Hours/Week		
						L	T	P
1	MJD 1	CSCY101	Digital Logic Fundamentals	H	4	3		2
2	MID 1	CSCY102	Networks Essentials	S	4	3		2
3	MLD 1		One course from the MLD streams (Table 10)	H	3	4		
4	AEC 1		English I / Modern Indian Language I	H	2	4		
5	SEC 1	CSCY103/ CSCY104	S.No. 1 or 2 from Table 7	S	3	2		2
6	VAC 1		Understanding India	H	2	4		
7	VAC 2		Environmental Science/ Education/Higher Order Thinking	H	2	4		
				Total	20	30 Hours		

SECOND SEMESTER								
S.No	Component	Course Code	Title of the Course	H/S	Credits	Hours/Week		
						L	T	P
1	MJD 2	CSCY105	Problem Solving and Programming Fundamentals	H	4	3		2
2	MID 2	CSCY106	Fundamentals of Cybersecurity	S	4	3		2
3	MLD 2		One course from the MLD streams except the stream chosen in MLD1 (Table 10)	H	3	4		
4	AEC 2		English I / Modern Indian Language I	H	2	4		
5	SEC 2	CSCY107/ CSCY108	S.No. 3 or 4 from Table 7	S	3	2		2
6	VAC 3		Health & Wellness/Yoga Education/Universal Human Values	H	2	2		2
7	VAC 4	COMS100	Digital Technologies	H	2	4		
				Total	20	30 Hours		

THIRD SEMESTER								
S.No	Component	Course Code	Title of the Course	H/S	Credits	Hours/Week		
						L	T	P
1	MJD 3	CSCY201	Object Oriented Programming	H	4	3		2
2	MJD 4	CSCY202	Data Structures	H	4	3		2
3	MID 3	CSCY203	Ethical Hacking	S	4	3		2
4	MLD 3		One course from the MLD streams except the streams chosen in MLD1 and MLD2 (Table 10)	H	3	4		
5	AEC 3		English II/ Modern Indian Language II	H	2	4		
6	SEC 3	CSCY204/ CSCY205	S.No. 5 or 6 from Table 7	S	3	2		2
				Total	20	27 Hours		

FOURTH SEMESTER								
S.No	Component	Course Code	Title of the Course	H/S	Credits	Hours/Week		
						L	T	P
1	MJD 5	CSCY206	Computer System Architecture	H	4	3		2
2	MJD 6	CSCY207	Design and Analysis of Algorithms	H	4	3		2
3	MJD 7	CSCY208	Database Management Systems	H	4	3		2
4	MID 4	CSCY209	Fundamentals of Cryptography	S	4	3		2
5	AEC 4		English II / Modern Indian Language II	H	2	4		
6	CES 1	CSCY210	Community Engagement and Service	H	2			6
				Total	20	30 Hours		

FIFTH SEMESTER								
S.No	Component	Course Code	Title of the Course	H/S	Credits	Hours/Week		
						L	T	P
1	MJD 8	CSCY301	Operating Systems	H	4	3		2
2	MJD 9	CSCY302	Mathematical Foundations of Computer Science	H	4	4	1	
3	MJD 10	CSCY303	Computer Networks	H	4	3		2
4	MID 5	CSCY304	Network Security	S	4	3		2
5	MJD 11	CSCY305	Summer Internship	H	4			6
				Total	20	26 Hours		

SIXTH SEMESTER								
S.No	Component	Course Code	Title of the Course	H/S	Credits	Hours/Week		
						L	T	P
1	MJD 12	CSCY306	Management Strategies and Concepts	H	4	5		
2	MJD 13	CSCY307	Software Engineering Theory and Practice	H	4	3		2
3	MJD 14	CSCY308	Distributed Systems	H	4	3		2
4	MJD 15	CSCY309	Operations Research	H	4	4	1	
5	MID 6	CSCY310/ CSCY311	Any one course from Table 1	S	4	4	1	
				Total	20	25 Hours		

SEVENTH SEMESTER								
S.No	Component	Course Code	Title of the Course	H/S	Credits	Hours/Week		
						L	T	P
1	MJD 16	CSCY401	Web Engineering	H	4	3		2
2	MJD 17	CSCY402	System Modeling and Simulation	H	4	3		2
3	MJD 18	CSCY403	Wireless Communication Networks	H	4	3		2
4	MID 7	CSCY404/ CSCY405	Any one course from Table 2	S	4	3		2
					(or)			
					4	4	1	
5	MID 8	CSCY406/ CSCY407	Any one course from Table 3	S	4	3		2
				Total	20	25 Hours		

EIGHTH SEMESTER – B.Sc. Cyber and Digital Sciences (Honors)								
S.No	Component	Course Code	Title of the Course	H/S	Credits	Hours/Week		
						L	T	P
1	MJD 19	CSCY408/ CSCY409	Any one course from Table 4	S	4	3		2
					(or)			
					4	4	1	
2	MJD 20	CSCY410/ CSCY411	Any one course from Table 5	S	4	3		2
					(or)			
					4	4	1	
3	MJD 21	CSCY412	Cybersecurity Risk Management	H	4	4	1	
4	MJD 22	CSCY413	Information Systems Audit	H	4	4	1	
5	MJD 23	CSCY414	Security Operation Centre	H	4	4	1	
				Total	20	25 Hours		

EIGHTH SEMESTER – B.Sc. Cyber and Digital Sciences (Honors with Research)								
S.No	Component	Course Code	Title of the Course	H/ S	Credits	Hours/Week		
						L	T	P
1	MJD 19	CSCY408/ CSCY409	Any one course from Table 4	S	4	3		2
					(or)			
					4	4	1	
2	MJD 20	CSCY410/ CSCY411	Any one course from Table 5	S	4	3		2
					(or)			
					4	4	1	
3	MJD 21	CSCY415	Research Project	H	4			5
4	MJD 22	CSCY416	Project Report	H	4			5
5	MJD 23	CSCY417	Project Viva-voce	H	4			5
				Total	20	25 Hours		

Table 1: MID 6 – SIXTH SEMESTER								
S.No	Component	Course Code	Title of the Course	H/S	Credits	Hours/Week		
						L	T	P
1	MID 6	CSCY310	Information Security Management	S	4	4	1	
2	MID 6	CSCY311	IoT and Security	S	4	4	1	

Table 2: MID 7 – SEVENTH SEMESTER								
S.No	Component	Course Code	Title of the Course	H/S	Credits	Hours/Week		
						L	T	P
1	MID 7	CSCY404	Digital Forensics	S	4	3		2
2	MID 7	CSCY405	Security Information and Event Management	S	4	4	1	

Table 3: MID 8 – SEVENTH SEMESTER								
S.No	Component	Course Code	Title of the Course	H/S	Credits	Hours/Week		
						L	T	P
1	MID 8	CSCY406	Machine Learning for Cybersecurity	S	4	3		2
2	MID 8	CSCY407	Threat Intelligence	S	4	3		2

Table 4: MJD 19 – EIGHTH SEMESTER								
S.No	Component	Course Code	Title of the Course	H/S	Credits	Hours/Week		
						L	T	P
1	MJD 19	CSCY408	Blockchain Technologies	S	4	3		2
2	MJD 19	CSCY409	Cyber Laws	S	4	4	1	

Table 5: MJD 20 – EIGHTH SEMESTER								
S.No	Component	Course Code	Title of the Course	H/S	Credits	Hours/Week		
						L	T	P
1	MJD 20	CSCY410	Database and Application Security	S	4	3		2
2	MJD 20	CSCY411	Data Privacy	S	4	4	1	

Table 6: MJD 21 / MJD 22 / MJD 23 – EIGHTH SEMESTER								
S.No	Component	Course Code	Title of the Course	H/S	Credits	Hours/Week		
						L	T	P
1	MJD 21	CSCY412	Cybersecurity Risk Management	S	4	4	1	
2	MJD 22	CSCY413	Information Systems Audit	S	4	4	1	
3	MJD 23	CSCY414	Security Operation Centre	S	4	4	1	

Table 7 : List of Skill Enhancement Courses/ SEC 1 / SEC 2 / SEC 3 – I / II / III SEMESTERs								
S.No	Component	Course Code	Title of the Course	H/ S	Credits	Hours/Week		
						L	T	P
1	SEC 1	CSCY103	Python Programming	S	3	3		2
2	SEC 1	CSCY104	Linux Programming	S	3	3		2
3	SEC 2	CSCY107	Network Traffic Analysis	S	3	3		2
4	SEC 2	CSCY108	Open Source Intelligence	S	3	3		2
5	SEC 3	CSCY204	Server Administration	S	3	3		2
6	SEC 3	CSCY205	Black Hat Python	S	3	3		2

Table 8: List of Major Disciplinary Courses				
S.No	Component	Course Code	Title of the Course	H/S
1.	MJD 1	CSCY101	Digital Logic Fundamentals	H
2.	MJD 2	CSCY105	Problem Solving and Programming Fundamentals	H
3.	MJD 3	CSCY201	Object Oriented Programming	H
4.	MJD 4	CSCY202	Data Structures	H
5.	MJD 5	CSCY206	Computer System Architecture	H
6.	MJD 6	CSCY207	Design and Analysis of Algorithms	H
7.	MJD 7	CSCY208	Database Management Systems	H
8.	MJD 8	CSCY301	Operating Systems	H
9.	MJD 9	CSCY302	Mathematical Foundations of Computer Science	H
10.	MJD 10	CSCY303	Computer Networks	H
11.	MJD 11	CSCY305	Summer Internship	H
12.	MJD 12	CSCY306	Management Strategies and Concepts	H
13.	MJD 13	CSCY307	Software Engineering Theory and Practice	H
14.	MJD 14	CSCY308	Distributed Systems	H
15.	MJD 15	CSCY309	Operations Research	H
16.	MJD 16	CSCY401	Web Engineering	H
17.	MJD 17	CSCY402	System Modeling & Simulation	H
18.	MJD 18	CSCY403	Wireless Communication Network	H
19.	MJD 19	CSCY408/ CSCY409	Blockchain Technologies / Cyber Laws	S
20.	MJD 20	CSCY410/ CSCY411	Database and Application Security / Data Privacy	S

Table 9: List of Minor Disciplinary Courses				
S.No	**Component**	**Course Code**	**Title of the Course**	**H/S**
1.	**MID 1**	**CSCY102**	**Network Essentials**	**S**
2.	**MID 2**	**CSCY106**	**Fundamentals of Cybersecurity**	**S**
3.	**MID 3**	**CSCY203**	**Ethical Hacking**	**S**
4.	**MID 4**	**CSCY209**	**Fundamentals of Cryptography**	**S**
5.	**MID 5**	**CSCY304**	**Network Security**	**S**
6.	**MID 6**	**CSCY310/ CSCY311**	**Information Security Management / IoT and Security**	**S**
7.	**MID 7**	**CSCY404/ CSCY405**	**Digital Forensics / Security Information and Event Management**	**S**
8.	**MID 8**	**CSCY406/ CSCY407**	**Machine Learning for Cybersecurity / Threat Intelligence**	**S**

*Table 10: MLD 1 / MLD 2 / MLD 3 in Sem 1 / Sem 2 / Sem 3			
Streams	**Course Code**	**Title of the Course**	**H/S**
Natural Science		Biology	**H**
		Botany	**H**
		Zoology	**H**
		Biotechnology	**H**
		Biochemistry	**H**
Physical Sciences		Chemistry	**H**
		Physics	**H**
		Biophysics	**H**
		Astronomy	**H**
		Astrophysics	**H**
		Earth and Environmental Sciences	**H**
Mathematics & Statistics		STATA	**H**
		SPSS	**H**
		Tally	**H**
Computer Science	**COMS101**	Introduction to Python Programming	**H**
	COMS102	Foundations of Information Technology	**H**
Social Sciences		Political Sciences	**H**
		History	**H**
		Social work	**H**
		Sociology	**H**
Humanities		Anthropology	**H**
		Psychology	**H**
		Economics	**H**
Commerce & Management		Business Management	**H**
		Accountancy	**H**
		Finance	**H**
		Financial Institutions	**H**
Media Sciences		Journalism	**H**
		Mass Media	**H**
		Communication	**H**

*Courses will be announced after the approval of the respective boards.

Table 11: List of Ability Enhancement Courses				
S.No	**Component**	**Course Code**	**Title of the Course**	**H/S**
1.	**AEC 1**		**English I/ Modern Indian Language I**	**H**
2.	**AEC 2**		**English I/ Modern Indian Language I**	**H**
3.	**AEC 3**		**English II / Modern Indian Language II**	**H**
4.	**AEC 4**		**English II/ Modern Indian Language II**	**H**

Table 12: List of Skill Enhancement Courses				
S.No	**Component**	**Course Code**	**Title of the Course**	**H/S**
1	**SEC 1**	**CSCY103**	**Python Programming**	**S**
2	**SEC 1**	**CSCY104**	**Linux Programming**	**S**
3	**SEC 2**	**CSCY107**	**Network Traffic Analysis**	**S**
4	**SEC 2**	**CSCY108**	**Open Source Intelligence**	**S**
5	**SEC 3**	**CSCY204**	**Server Administration**	**S**
6	**SEC 3**	**CSCY205**	**Black Hat Python**	**S**

Table 13: List of Value-Added Courses				
S.No	**Component**	**Course Code**	**Title of the Course**	**H/S**
1.	**VAC 1**		**Understanding India**	**H**
2.	**VAC 2**		**Environmental Science/ Education / Higher Order Thinking**	**H**
3.	**VAC 3**		**Health & Wellness / Yoga Education / Universal Human Values**	**H**
4.	**VAC 4**	**COMS100**	**Digital Technologies**	**H**

Table 14: Project (WP/ Internship)				
S.No	**Component**	**Course Code**	**Title of the Course**	**H/S**
1.	**Project**	**CSCY210**	**Community Engagement and Service**	**H**

B.Sc. Cyber and Digital Sciences

SYLLABUS

SEMESTER I

Year	I	Course Code: CSCY101	Credits	4
Sem.	I	Course Title: Digital Logic Fundamentals	Hours	75
			Category	C
Course Prerequisites, if any	● Basic knowledge of Computers			
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory): 03 hrs. Duration of ESA (Practical): 03 hrs.		
Course Outcomes	● Understand and describe the principles of digital systems and binary number operations ● Apply Karnaugh mapping to simplify Boolean expressions and optimize digital circuits ● Analyze and design basic combinational circuits using various digital components ● Synthesize and evaluate synchronous sequential circuits using storage elements and HDL ● Design and implement various types of registers and counters using HDL			
Unit No.	**Course Content**		**Hours**	
Theory Component				
Unit I	**Digital Systems and Binary Numbers** Digital Systems – Binary Numbers – Number-Base Conversions – Octal and Hexadecimal Numbers – Complements of Numbers – Signed Binary Numbers – Binary Codes – Binary Storage and Registers – Binary Logic – Axiomatic Definition of Boolean Algebra – Basic Theorems and Properties of Boolean Algebra – Boolean Functions – Canonical and Standard Forms – Other Logic Operations – Digital Logic Gates – Integrated Circuits		9	
Unit II	**Gate-Level Minimization** Map Method – Four-Variable K-Map – Product-of-Sums Simplification – Don't-Care Conditions – NAND and NOR Implementation – Other Two-Level Implementations – Exclusive-OR Function – Hardware Description Language		9	
Unit III	**Combinational Logic** Analysis Procedure – Design Procedure – Binary Adder–Subtractor – Decimal Adder – Binary Multiplier – Magnitude Comparator – Decoders – Encoders – Multiplexers – HDL Models of Combinational Circuits		9	
Unit IV	**Synchronous Sequential Logic** Storage Elements – Latches – Flip-Flops – Analysis of Clocked Sequential Circuits - Synthesizable HDL Models of Sequential Circuits – State Reduction and Assignment – Design Procedure		9	
Unit V	**Registers and Counters** Registers – Shift Registers – Ripple Counters – Synchronous Counters – Other Counters – HDL for Registers and Counters		9	
Practical Component				
	1. Binary to Decimal and vice-versa in Python 2. Decimal to Hexadecimal and Vice-Versa in Python 3. Digital Logic Gates in Python			

Exercises	4. Simplification of Boolean Functions in Python 5. Combinational Logic Circuits in Python i. Code Converters ii. Arithmetic (Adders, Subtractors, Multipliers, Comparators) iii. Data Handling (Multiplexers, Demultiplexers, Encoders & Decoders) 6. Combinational Logic Circuit Design in Python 7. Binary Adder-Subtractor Simulation in Python 8. Decimal Adder Simulation in Python 9. Binary Multiplier Simulation in Python 10. Sequential Circuit Storage Elements: Flip-Flop Simulation in Python	30
Recommended Learning Resources		
Print Resources	1. M. Morris Mano, Michael D. Ciletti, "Digital design with an introduction to the Verilog HDL", Pearson, Sixth Edition, 2018. 2. M. Rafiquzzaman, "Fundamentals of Digital Logic and Microcomputer Design", John Wiley & Sons, Inc., Fifth Edition, 2009.	
Syllabus design: Dr. M.Sathya, Assistant Professor, PUDoCS		

Year	I	Course Code: CSCY102	Credits	4
Sem.	I	Course Title : Network Essentials	Hours	75
			Category	C
Course Prerequisites, if any	● Knowledge of computers			
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory): 03 hrs. Duration of ESA (Practical): 03 hrs.		
Course Outcomes	● Understanding the basics of digital communication, network models and internetworking devices ● Learning about LAN, Internet, Intranet and Extranet ● Learning about the various network technologies ● Analyzing and resolving connectivity problems ● Evaluating the potential impact of new technologies on network design			
Unit No.	**Course Content**		**Hours**	
Theory Component				
Unit I	**Network Models, Cabling and Topology** The TCP/IP Model- The Link layer, The Internet layer, The Transport Layer, The Application Layer, Frames Packets and Segments-Topology- Bus and Ring, Star, Hybrids, Mesh and Point to Multipoint, Point-to-Point,Parameters of Topology-Cabling - Coaxial cable, Twisted Pair, Fiber-optic,other cables, Fire ratings		9	
Unit II	**Installing a Physical Network and TCP/IP Basics** Structured Cabling, Installing Structured Cabling, NICs, Diagnostics and Repair of Physical Cabling - Standardizing Networking Technology, The TCP/IP Protocol Suite, IP in Depth, CIDR and Subnetting, Using IP Addresses		9	
Unit III	**TCP/IP Applications and Network Naming** Transport Layer and Network Layer Protocols, Port Numbers, Communication TCP/IP Application – DNS(Domain Name System), WINS, Diagnosing TCP/IP Networks		9	
Unit IV	**Protecting Network** Common Threats- System Crash/ Hardware Failure, Administrative Access Control, Malware, Social Engineering, Man in the middle, Denial of Service, Physical Intrusion, Attacks on wireless Connections - Securing User Accounts-Authentication, Passwords, Controlling User Accounts-Firewalls- Hiding the IPs, Port Filtering,Packet Filtering, MAC filtering, Personal Firewalls, Network Zones and Vulnerability Scanners		9	
Unit V	**Network Troubleshooting** Troubleshooting Tools, The Troubleshooting Process, Identify the Problem, Establish a Theory of Probable Cause, Test the Theory to Determine Cause, Establish a Plan of Action and Identify Potential Effects, Implement and Test the Solution or Escalate as Necessary, Verify Full System Functionality and Implement Preventative Measures, Document Findings, Actions, and Outcomes, Troubleshooting Scenario		9	
Practical Component				

Exercises	1. Configure NIC settings (IP address, subnet mask, gateway) a. Use ping to test connectivity. b. Use ethtool to diagnose NIC issues on Linux. 2. Perform the IP address configuration (static and dynamic) of a computer system 3. Perform the DHCP configuration of a computer system 4. Configure MS outlook to receive emails from email accounts in different mail servers 5. Use *telne*t and *ftp* commands to establish a remote connection and transfer files 6. Execute netstat command with all of its parameters and record the results 7. Query DNS records using all DNS commands 8. Configure the firewall settings for a computer system and also create firewall rules with *iptables* and *netsh advfirewa*ll to block/allow specific traffic 9. Troubleshoot network connectivity issues using *ping, tracert/traceroute, and ipconfig/ifconfig* 10. Install and configure a network operating system. Create user groups and user accounts in each group with appropriate account settings. Enable file and printer sharing among the user groups	30
Recommended Learning Resources		
Print Resources	1. Mike Meyers. " CompTIA Network+ Guide to Managing and Troubleshooting Networks", 7th Edition,McGraw-Hill Education, 2022. 2. Jan L. Harrington. "Ethernet Networking for the Small Office and Professional Home Office-Morgan Kaufmann", Elsevier, 2007. 3. Behrouz A. Forouzan, "Data communication and Networking", 4th Edition, McGraw-Hill, India, 2017. 4. Palmer, M., "Hands-on networking fundamentals", Cengage learning, 2012.	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

Year	I	Course Code: CSCY103	Credits	3
Sem.	I	Course Title : Python Programming	Hours	60
			Category	B
Course Prerequisites, if any	● Basic Knowledge of Programming			
Internal Assessment Marks: 50	End Semester Marks: 50	Duration of ESA (Practical) : 03 hrs.		
Course Outcomes	• Understand the basics of writing Python code • Implement programs using lists, tuples and dictionaries • Understand the use of control structures • Implement programs using packages • Understand the file manipulation			

Unit No.	Course Content	Hours
	Theory Component	
Unit I	**Introduction, Data types** Introduction to Python – Advantages of using Python – Executing Python Programs – Python's Core data types – Numeric Types – String Fundamentals.	6
Unit II	**Lists, Tuples, Dictionaries** Lists: list operations, list slices, list methods, list loop, mutability, aliasing, cloning lists, list parameters; Tuples: tuple assignment, tuple as return value; Dictionaries: operations and methods; advanced list processing – list comprehension.	6
Unit III	**Control Flow, Functions, Modules** Python Statements: Assignments – Expressions – If condition – While and For Loops. Functions: Definition, Calls – Scopes – Arguments – Recursive Functions– Functional Programming tools. Classes and Object Oriented programming with Python - Modules and Packages: Purpose, using packages– Exception Handling with Python.	6
Unit IV	**Packages** Packages: NumPy, Pandas, Scikit learn - Machine learning with Python – Cleaning up, Wrangling, Analysis, Visualization - Matplotlib package – Plotting Graphs	6

Unit V	**File Handling** Files and exception: text files, reading and writing files, format operator; command line arguments, errors and exceptions, handling exceptions	6
Practical Component		
Exercises	1. Exchange the values of two variables 2. Finding minimum among n variables 3. Perform Simple sorting 4. Generate Students marks statement 5. Find square root, GCD, exponentiation 6. Sum the array of numbers 7. Perform linear search, binary search 8. Perform Matrix operations using NumPy 9. Perform Dataframe operations using Pandas 10. Use Matplotlib on dataset and visualize 11. Perform Word count, copy file operations	30
Recommended Learning Resources		
Print Resources	1. Mark Lutz, "Learning Python", Fifth Edition, O'Reilly, 2013. 2. Daniel Liang, "Introduction to programming using Python", Pearson, First edition, 2021. 3. Wes Mc Kinney, "Python for Data Analysis", O'Reilly Media, 2012. 4. Tim Hall and J-P Stacey, "Python 3 for Absolute Beginners", Apress, First Edition, 2009. 5. Magnus Lie Hetland, "Beginning Python: From Novice to Professional", Apress, Second Edition, 2005.	
Syllabus design: Dr.V.Uma, Associate Professor, PUDoCS		

Year	I	Course Code: CSCY104	Credits	3
			Hours	60
Sem.	I	Course Title : Linux Shell Programming	Category	B
Course Prerequisites, if any	● Basic knowledge of computers and programming			
Internal Assessment Marks: 50	End Semester Marks: 50	Duration of ESA (Practical) : 03 hrs.		
Course Outcomes	● Learning commands of linux operating system ● Understanding the concepts of shell programming ● Understanding the use of quotes, backslash, command substitution and passing arguments ● Learning to work with decisions and loops ● Creating shell programs to demonstrate the reading and printing of data			

Unit No.	Course Content	Hours
	Theory Component	
Unit I	**Introduction to Linux Commands and Shell** Basic commands, working with files, working with directories, file name substitution, file name nuances, Standard input / Output and I/O redirection, pipes, standard error, advanced commands – kernel and the utilities, login shell, typing commands to the shell, the shell's responsibilities	6
Unit II	**Regular Expressions, Commands, Command files and Variables** Various ways of forming regular expressions, cut, paste, sed, tr, grep sort, uniq commands and their various options, command files, variables – displaying values of variables, undefined variables, file name substitution and variables, $ construct, built-in integer arithmetic	6
Unit III	**Use of Quotes, Backslash, command substitution and passing arguments** Single quote, double quote, backslash, command substitution, passing arguments, example programs, shift command	6
Unit IV	**Decisions and Loops** Exit Status, test command, else construct, exit command, elif construct, case command, Null Command, && and || constructs – for, while and util loops, advanced loops, getopts commands	6
Unit V	**Reading and Printing data and Interactive and Non-standard shell features** Read command, printf command, getting the right shell, the ENV file, command-line editing, Command history, vi line edit mode, emacs line edit mode, accessing history, functions, integer arithmetic, alias command, arrays, job control, miscellaneous features	6
	Practical Component	
	1. Demonstrating the use of all linux commands 2. Demonstrating the use of typing commands to the shell. 3. Demonstrating the formation of regular expressions using various options 4. Using cut, paste, sed, tr, grep, sort and uniq commands 5. Demonstrating the use of variables, and built-in arithmetic 6. Demonstrating the use of single, double quotes, backslash, commands substitution	30

Exercises	7. Demonstrating the passing of arguments 8. Creating shell programs to demonstrate the use of decision commands 9. Creating shell programs to demonstrate various kinds of loops 10. Creating shell programs to demonstrate the reading and printing of data 11. Demonstration of Command-Line editing, command history, vi and emacs line edit mode, history command, alias command, etc.	
Recommended Learning Resources		
Print Resources	1. Stephen J. Kochan, Patrick Wood, "Shell programming in Unix, Linux and OS X", Addison Wesley publication, 2017. 2. Mark G. Sobell, "Linux, Commands, Editors, Shell Programming", Third edition, Prentice Hall, 2012.	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

SEMESTER II

<table>
<tr><td>Year</td><td>I</td><td colspan="2" rowspan="2">Course Code: CSCY105

Course Title: Problem Solving & Programming Fundamentals</td><td>Credits</td><td>4</td></tr>
<tr><td rowspan="2">Sem.</td><td rowspan="2">II</td><td>Hours</td><td>75</td></tr>
<tr><td>Category</td><td>C</td></tr>
<tr><td>Course Prerequisites, if any</td><td colspan="4">● Basic knowledge of Computers</td></tr>
<tr><td>Internal Assessment Marks: 25</td><td colspan="2">End Semester Marks: 75</td><td colspan="2">Duration of ESA (Theory): 03 hrs.
Duration of ESA (Practical): 03 hrs.</td></tr>
<tr><td>Course Outcomes</td><td colspan="4">● Analyze problems and develop top-down designs
● Write, compile, and debug basic programs
● Implement logic with conditionals and loops
● Manipulate arrays of various dimensions
● Design and implement functions with recursion</td></tr>
<tr><td>Unit No.</td><td colspan="3">Course Content</td><td>Hours</td></tr>
<tr><td colspan="5">Theory Component</td></tr>
<tr><td>Unit I</td><td colspan="3">Introduction to Computer Problem-Solving
Problem-solving Aspect – Top-down Design – Implementation of Algorithms – Program Verification – Efficiency of Algorithms – Analysis of Algorithms</td><td>9</td></tr>
<tr><td>Unit II</td><td colspan="3">Basic programming constructs
Basic Data types (Numerical, String) – Variables – Expressions – I/O statements – Compile and Run – Debugging</td><td>9</td></tr>
<tr><td>Unit III</td><td colspan="3">Decision Making – Branching & Looping
Decision making – Relational Operators – Conditional statement, Looping Statements – Nested loops – Infinite loops – Switch Statements</td><td>9</td></tr>
<tr><td>Unit IV</td><td colspan="3">Array Techniques
Array Manipulation – Different operations – One dimensional Array – Two-dimensional Array – Multi-dimensional Array – Character – Arrays and Strings</td><td>9</td></tr>
<tr><td>Unit V</td><td colspan="3">Modular solutions
Introduction to Functions – Importance of Design of Functions – Arguments – Parameters – Return Values – Local and Global Scope – Recursion</td><td>9</td></tr>
<tr><td colspan="5">Practical Component</td></tr>
<tr><td>Exercises</td><td colspan="3">1. Program to array counting, array order reversal & find the maximum number in a set
2. Program for removal of duplicates from an ordered array & to partition an array
3. Program to find the k^{th} smallest element
4. Program to exchange the values of two variables without using a third variable
5. Program that takes a list of numbers as input and counts the total number of elements in the list
6. Program to compute the factorial of a given integer
7. Program to compute the sine of an angle (in degrees) using a series expansion</td><td>30</td></tr>
</table>

	8. Program to generate the Fibonacci sequence up to a specified limit 9. Program that takes an integer as input and reverses its digits 10. Program that converts a number from one base to another (e.g., binary to decimal, decimal to binary)	
Recommended Learning Resources		
Print Resources	1. R. G. Dromey, "How to Solve it by Computer", Pearson Education India, Thirteen Edition, 2013. 2. Allen B. Downey, "Think Python: How to Think like a Computer Scientist", Third Edition, O'Reilly Publishers, 2020.	
Syllabus design: Dr. M.Sathya, Assistant Professor, PUDoCS		

Year	I	Course Code: CSCY106	Credits	4
Sem.	II		Hours	75
		Course Title: Fundamentals of Cybersecurity	Category	C
Course Prerequisites, if any	● Basic knowledge of computer networks and internet			
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory) : 03 hrs. Duration of ESA (Practical) : 03 hrs.		
Course Outcomes	● Learning the basic concepts of cybersecurity ● Understanding user authentication and access control ● Comprehending the basics of cryptography ● Obtaining a basic knowledge of cyber laws and regulations ● Understanding operating system and network security principles			

Unit No.	Course Content	Hours
	Theory Component	
Unit I	**Introduction to Computer and Information Security** Foundation of Computer and Information Security: Definition and its needs, Triad and Parkerian Hexad security models and issues- Attacks and its types – Threats, vulnerabilities and Risk - risk management – Incident response and Defense in depth.	9
Unit II	**User Authentication and Access Control** Understanding Identification, Authentication and Authorization, Identity verification, Falsifying Identification – Authentication factors – Multifactor and Mutual authentication – Common Identification and Authentication methods – ACL and its capabilities – Access Control Models – DAC, RBAC, ABAC, MAC – Physical Access control - Auditing and Accountability – Non Repudiation, Deterrence, IDS and IPS, Logging, Monitoring and audit with assessments.	9
Unit III	**Cryptography** History of Cryptography-Caesar Cipher, Cryptographic Machines, kerckhoffs's Principles – Modern Tools – Cipher, OTP, Symmetric and Asymmetric cryptography, Hash Function, Digital Signature, Certificate – Protecting data at Rest, in Motion, and in Use.	9
Unit IV	**Compliance, Laws, regulation and Operation security** Types of compliance and is Consequences – Achieving and maintaining compliance with control, Government and Industry related regulatory – Adopting compliance frameworks, Compliance and technological changes in cloud, Blockchain and cryptocurrencies - Process of operation security, its effect in personal lives and origins, Laws of Operation security.	9
Unit V	**Network and Operating System Security** Human element Security – Gathering information for Social Engineering Attacks and its types, building security awareness – Physical threat Identification and control, Protecting- people, data and equipment – Designing secure network using firewall and IDS – Protecting Network traffic using network security tools – OS hardening – Protecting against Malware – OS security tools for scanning and	9

	assessment of vulnerability – Mobile, Embedded, IoT and application Security.	
Practical Component		
Exercises	1. Perform a survey of various malware attacks that have happened in the last 3 years, the industry in which it had happened, the losses incurred, the data that was breached and prepare a report on the same. 2. Identify some open source malware creation tools (virus, worms, etc. creation tools) and create the corresponding malware. 3. Study the various authentication methods and prepare report on a comparison of the authentication methods. 4. Providing use case scenarios of the various authentication methods that are used in real life. 5. Using online cryptography tools, create ciphers using symmetric and symmetric cryptography. 6. Create message digest using online hash function, create a digital certificate online 7. Perform a study of cybersecurity laws in India, USA and UK and compare them. 8. Perform a study of open source firewall and IDS tools 9. Install and work with tcpdump commands in linux 10. Demonstrate OS hardening.	30
Recommended Learning Resources		
Print Resources	1. Jason Andress, “Foundations of Information Security - A Straightforward Introduction” , William Pollock Publisher, 2019. 2. Atul Kahate, , “Cryptography and Network Security”, McGraw Hill Education, 2019. 3. Harish Chander and Gagandeep Kaur, “Cyber Laws and IT Protection”, PHI Publication, 2022. 4. Alan Calder, “Implementing Information security based on ISO 27001/ISO 27002 (Best Practice)”, Van Haren Publishing, 2009.	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

Year	I	Course Code: CSCY107	Credits	3
Sem.	II		Hours	60
		Course Title : Network Traffic Analysis	Category	B
Course Prerequisites, if any	● Basic knowledge of computers, networks and internet			
Internal Assessment Marks: 50	End Semester Marks: 50	Duration of ESA (Practical) : 03 hrs.		
Course Outcomes	● Being able to install and configure network traffic analysis tool ● Understanding the basics of network traffic capture and filtered view of packets ● Learning to interpret network traffic from packets ● Obtaining knowledge of display filters and packet reassembling ● Analyzing TCP/IP protocols traffic viz., DNS, ARP, ICMP, DHCP, TCP, UDP, HTTP and Email traffic			

Unit No.	Course Content	Hours
	Theory Component	
Unit I	**IP Addressing and TCP/IP protocols** Logical Addressing, IPV4 Addresses, Classful addressing, subnetting, supernetting, Classless addressing, Hierarchy, Network Address Translation, Network Layer Protocols – TCP, UDP, ICMP, ARP, RARP, DHCP, Application Layer Protocols – DNS, SMPT, POP and IMAP.	6
Unit II	**Capturing, Viewing and Interpreting Traffic** Introduction to Network Analysis, Introduction to Wireshark, Capturing traffic, Creating and applying packet filters, defining global and personal preferences, Colorizing traffic, defining time values and interpreting summaries, interpreting basic trace file statistics.	6
Unit III	**Display Filter and Packet Reassembling** Creating and applying display filters, Following streams and reassembling data, customizing Wireshark profiles, customizing profiles.	6
Unit IV	**TCP IP Protocols Analysis - I** TCP/IP Analysis overview, Analyzing DNS traffic, ARP traffic, IPV4 traffic, ICMP traffic.	6
Unit V	**TCP IP Protocols Analysis - II** Analyzing UDP traffic, TCP traffic, DHCP traffic, HTTP traffic, Email traffic.	6
	Practical Component	
Exercises	1.Perform hands-on exercises relating to IP addressing, subnetting, supernetting. 2. Perform hands-on exercises relating to capturing traffic, packet filters. 3. Perform hands-on exercises on setting preferences colorizing traffic and defining time values. 4. Perform hands-on exercises on interpreting summaries and interpreting basic trace file statistics.	30

	5. Perform hands-on exercises relating to creating and applying display filters. 6 Perform hands-on exercises on following streams and reassembling data 7. Perform hands-on exercises on customizing wireshark profiles, customizing profiles. 8. Perform hands-on exercises relating to analyzing DNS traffic, ARP traffic ,IPV4 traffic, ICMP traffic. 9. Perform hands-on exercises relating to analyzing UDP traffic. 10. Perform hands-on exercises relating to analyzing TCP traffic Open Source used : Wireshark	
Recommended Learning Resources		
Print Resources	1. Behrouz A. Forouzan, "Data Communications and Networking", Mc Graw Hill Education, 2017. 2. Vinit Jain, " Wireshark Fundamentals: A Network Engineer's Handbook to Analyzing Network Traffic", Apress Publishing, 2022. 3. Chris Sanders, "Practical Packet Analysis – Using Wireshark to solve real world network problems", No Starch Press Publishing, 2011	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

Year	I	Course Code: CSCY108	Credits	3
Sem.	II	Course Title: Open Source Intelligence	Hours	60
			Category	B
Course Prerequisites, if any	● Basic knowledge of computer networks and internet			
Internal Assessment Marks: 50	End Semester Marks: 50	Duration of ESA (Practical) : 03 hrs.		
Course Outcomes	● Understanding the basics of Open Source Intelligence, Online Threats and its Countermeasures ● Gaining knowledge on underground Internet and using search engine techniques to gather required information ● Being able to perform social medial intelligence, using people search engines, and searching public records ● Analyzing possible information from online maps ● Creating Technical footprinting			

Unit No.	Course Content	Hours
	Theory Component	
Unit I	**Introduction to Open Source Intelligence, Online Threats and Countermeasures** Open Source information categories, OSINT Types, OSINT organizations, parties interested in OSINT, Information Gathering types, Benefits of OSINT, challenges of OSINT, legal and ethical constraints - Online Threats, security software, securing the operating system, General privacy settings, Online tracking techniques, Secure online browsing, Secure online communication, online anonymity, encryption techniques	6
Unit II	**Underground Internet and Search Engine Techniques** Layers of the internet, Darknet users, using Tor, Searching the Tor network – Key discovery and research, Using search engine to locate information, Web directories, web directories, Translation services, website history and website capture, website monitoring services, news search, searching for digital files	6
Unit III	**Social Media intelligence, people search engines and public records** Social media intelligence, social media content types, classification of social media platforms, popular social networking sites, investigating social media sites, general resources for locating information on social media sites, other social media sites, Pastebin sites, social media psychological analysis, people search engine, public records, examples, searching for personal details – general, online registries, vital records, criminal and court search, property records, tax and financial records, SSN search, username check, email search, data compromised repositories, phone number search, employee profiles and job websites, other public records.	6
Unit IV	**Online Maps** The basics of geolocation tracking, finding GPS coordinates of any location on a map, finding geo coordinates from a mailing address –	6

	general geospatial research tools – commercial satellites, date/time around the world, location based social media, YouTube, Facebook, Twitter, other social media platforms, conducting location searches on social media, country profile information, transport tracking, package tracking, webcams, digital file metadata	
Unit V	**Technical Footprinting** Investigating the target website, investigate the Robot.txt file, mirror the target website, extract the links, checking the target website's backlinks, monitor the website updates, checking the website archived contents, identifying the technologies used, web scraping tools, investigating the target website's File metadata, website certification search, website statistics and analytics tools, website reputation checker tools, passive technical reconnaissance activities – WHOIS lookup, subdomain discovery, DNS reconnaissance, IP address tracking	6
Practical Component		
Exercises	1. Demonstrating securing of operating systems 2. Demonstrating privacy settings and online tracking in a browser 3.Demonstrating secure online browsing, secure online communication and online anonymity 4. Demonstrating the use of encryption techniques. 5. Demonstrating with suitable examples the use of searching the Tor network, Key discovery and research 6. Demonstrating the Use of search engines to locate information 7. Demonstrating the Use of search engine to locate Web directories, Translation services, website history and website capture 8. Demonstrating the website monitoring services, news search, searching for digital files 9. Demonstrating with suitable examples - investigation of social media sites, locating information on social media sites, social media psychological analysis 10. Demonstrating with suitable examples people search engine, searching public records, searching for personal details, general details , searching online registries, vital records, performing criminal and court search, searching property records, tax and financial records, performing SSN search, username check, email search, data compromised repositories, phone number search, employee profiles and job websites, other public records search Open Source used : Maltego, shodan, Recon-ng, Google Dorks, theHarvester	30
Recommended Learning Resources		
Print Resources	1. Nihad A. Hassan, Rami Hijazi, "Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence", Apress Publisher, 2018. 2. Sudanshu Chauhan, Nutan Kumar Panda, " Hacking Web Intelligence: Open Source Intelligence, and Web Reconnaissance Concepts and Techniques", Syngress Publisher, 2015.	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

Year	I	Course Code: COMS100	Credits	2
Sem.	II	Course Title: Digital Technologies	Hours	45
			Category	A

Course Prerequisites, if any	● Basic knowledge of computers, networks and internet	
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory) : 03 hrs.
Course Outcomes	● Get introduced to the digital systems and its building blocks ● Understand how Digital Communication happens and to Learn the advantages and disadvantages including Cybersecurity ● Learn the day to day digital activities and the initiatives on Digital India ● Acquire knowledge on current Technologies and Trends in Digital Space ● Explore the applications on the state of the art in Digital Technologies	

Unit No.	Course Content	Hours
	Theory Component	
Unit I	**Introduction** Digital Systems - Information & Communication Technology - ICT Tools. Computer Architecture – Software – Hardware - Operating System - Algorithms - Flowcharts.	7
Unit II	**Communication Systems** Transmission Media - Computer Networks – Internet - Web Browsers - Search Engines - Messaging, Email - Social Media – Online Ethics. **Cybersecurity:** Threats, Significance, Challenges, Precautions, Safety Measures. Cyber Crime Awareness.	7
Unit III	**Digital India & e-Governance** Initiatives - Unified Payment Interface - Aadhar online services - Credit / Debit Cards - e-Wallets – Mobile and Internet Banking – NEFT / RTGS / IMPS - Online Payments & PoS - Digital Accessibility.	7
Unit IV	**Emerging Technologies & Applications: (Basic introduction only)** Overview of Artificial Intelligence, Cloud Computing, Big Data, Internet of Things, Virtual Reality, 5G, 3D Printing.	7
Unit V	**Case Studies** Any one case study on the emerging technologies and report submission by the candidates.	7
	Practical Component	
Practice	1. Operating System Installation and configuration 2. Application Software Installation and configuration 3. Hardware understanding and minor troubleshooting 4. Networking, cabling, configuration	10
	Recommended Learning Resources	
Print Resources	1. Pramod Kumar, Anuradha Tomar, R. Sharmila, "Emerging Technologies in Computing - Theory, Practice, and Advances", Chapman and Hall / CRC, 1st Edition, 2021, eBook ISBN: 9781003121466. https://doi.org/10.1201/9781003121466.	

	2. V. Rajaraman, “Introduction to Information Technology”, PHI, 3rd Edition, 2018, ISBN-10: 9387472299, ISBN-13: 978-9387472297. 3. E. Balagurusamy, “Fundamentals of Computers”, Tata Mc GrawHill, 2nd Edition, 2011, ISBN: 9780071077880. 4. Behrouz A. Forouzan, “Data Communications and Networking”, McGraw Hill, 4th Edition, 2007, ISBN 978-0-07-296775-3. 5. Rajkumar Buvya, James Broberg, and Andrzej Gosciniski, “Cloud Computing-Principles and Paradigms”, Wiley, 2011, ISBN: 978-0-470-88799-8. 6. Stuart Russel and Peter Norvig, “Artificial Intelligence - A Modern Approach”, Pearson Education, 3rd Edition, 2010, ISBN- 13: 978-0-13 -604259-4. 7. Samuel Greengard, “Internet of Things”, The MIT Press, 2015, ISBN: 9780262328937, https://doi.org/10.7551/mitpress/10277.001.0001. 8. C.S.V. Murthy, “E- Commerce – Concept, Models & Strategies”, Himalaya Publishing House, 2015, ISBN: 8178662760. 9. Hurwith, Nugent Halper, Kaufman, “Big Data for Dummies”, Wiley & Sons, 1st Edition, 2013, ISBN-13: 978-1118504222.
Syllabus Design: Prof. S.K.V. Jayakumar, Professor, PUDoCS	

SEMESTER III

Year	II	Course Code: CSCY201 Course Title: Object Oriented Programming	Credits	4
Sem.	III		Hours	75
			Category	C
Course Prerequisites, if any	● Basic knowledge of Programming			
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory): 03 hrs. Duration of ESA (Practical): 03 hrs.		
Course Outcomes	● Understand the principles of OOP and the concept of class and objects ● Apply the concept of Object initialization and overloading ● Understand the concept of inheritance and reusability ● Understand file operations and exception handling ● Apply OOP to design and implement solutions to real-world problems			

Unit No.	Course Content	Hours
	Theory Component	
Unit I	**Principles of Object Oriented Programming (OOP)** Object Oriented Programming Paradigm-Basic Concepts of OOP-Benefits of OOP - Application of OOP - Simple C++ program - Compiling and Linking	9
Unit II	**Classes and Objects** Specifying class - Member functions - Nesting of Member functions - Access specifier - Static Data members and functions - Arrays within a Class - Arrays of Objects - Objects as Arguments - Returning Objects - Friend Function	9
Unit III	**Object Initialization and Overloading** Types of Constructors - Dynamic Initialization of Objects - Destructors Operator overloading - function Overloading - Manipulation of Strings	9
Unit IV	**Inheritance** Derived Classes - Types of inheritance - Virtual Base Classes - Abstract Classes - Pointers to Derived Classes - Virtual base class - Method Overriding - Pure Virtual Functions	9
Unit V	**File operations and Exception handling** Classes for File Operations - File Modes - opening and closing a File - Basics of Exception Handling - Try-Catch block - Case Studies on Real Time Applications	9
	Practical Component	
Exercises	1. Write a Program to Read and Print Number Input From the User 2. Write a simple program using a class and objects 3. Write a program to demonstrate the usage of a constructor and destructor in a class 4. Write a program to overload + operator to add two complex numbers 5. Write a program to demonstrate the usage of function overloading 6. Write a program to display employee information using multiple inheritance 7. Write a program to demonstrate multilevel inheritance	30

	8. Write a program to copy a file from one location to another location	
Recommended Learning Resources		
Print Resources	1. E Balagurusamy, “Object oriented Programming with C++”, Seventh edition, Tata McGraw Hill, 2020.	
Syllabus Design: Dr. T. Vengattaraman, Associate Professor, PUDoCS		

Year	II	Course Code: CSCY202	Credits	4
Sem.	III	Course Title: Data Structures	Hours	75
			Category	C
Course Prerequisites, if any	● Basic knowledge of Computing			
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory): 03 hrs. Duration of ESA (Practical): 03 hrs.		
Course Outcomes	● Learn basic terminologies of linear and nonlinear data structures and algorithms ● Understand the concept of polynomial addition and sparse matrices using arrays ● Apply linked lists to solve problems related to stacks, queues, and sparse matrices ● Understand the operations and traversals of binary trees ● Apply graph algorithms to solve problems like topological sorting and finding minimum cost spanning trees			

Unit No.	Course Content	Hours
	Theory Component	
Unit I	**Introduction** Basic terminologies – Linear and Nonlinear data structures. Algorithm: Definition – Pseudo code – Analysis – Design Techniques.	7
Unit II	**Arrays, Stacks and Queues** Representation – Polynomial Addition – Sparse Matrices – Multidimensional Arrays. Stacks and Queues**:** Stack ADT – Operations – Evaluation of Expressions – Queue ADT – Operations – Application – Multiple Stacks and Queues	11
Unit III	**Lists** Singly Linked Lists – Linked Stacks and Queues – Operations – Circularly Linked Lists – Equivalence Relations – Sparse Matrices – Doubly Linked Lists	9
Unit IV	**Trees** Basic Terminologies – Binary trees – Representation, Operations, Traversals, Types – Applications of Trees	9
Unit V	**Graphs** Basic Terminologies – Representation, Operations, Traversals – Applications - Shortest path problem, Topological sorting, Minimum Cost Spanning trees	9
	Practical Component	
Exercises	1. Searching Algorithms (with the number of key comparisons) - Sequential, Binary and Fibonacci search algorithms 2. Evaluation of arithmetic expression 3. Stack, Queue, Circular queue, priority queue 4. Singly Linked List, Doubly Linked List, Circular Linked List	30

	5. Tree Traversal techniques 6. Graph Traversal techniques 7. Dijkstra's Algorithm to obtain the shortest paths	
Recommended Learning Resources		
Print Resources	1. Ellis Horowitz, Sartaj Sahni, Susan Anderson-Freed, Fundamentals of Data Structures in C", India University Press, Second Edition, 2008. 2. Debasis Samanta, "Classic Data Structures", Prentice-Hall of India, Pvt. Ltd., India, Seventeenth Printing, Second Edition, 2009. 3. Dinesh P Mehta & Sartaj Sahni, Handbook of Data Structures and Applications, Second Edition, Chapman and Hall, 2020.	
Syllabus design: Dr. M.Sathya, Assistant Professor, PUDoCS		

Year	II	Course Code: CSCY203	Credits	4
Sem.	III	Course Title : Ethical Hacking	Hours	75
			Category	C

Course Prerequisites, if any	● Basic Understanding of networks and internet		
Internal Assessment Marks: 25	End Semester Marks: 75		Duration of ESA (Theory): 03 hrs. Duration of ESA (Practical): 03 hrs.
Course Outcomes	● Understand the basic concepts of ethical hacking ● Learn the various phases of ethical hacking ● Learning the various tools related to every phase of ethical hacking ● Applying the tools to perform the various ethical hacking tasks ● Learn the countermeasures to prevent hacking		

Unit No.	Course Content	Hours
	Theory Component	
Unit I	**Ethical Hacking and Security Foundations** Overview of Ethics, Overview of Ethical Hacking, Methodologies, Methodology of Ethical Hacking **-** Security Foundations - The Triad, Risk, Policies Standard and Procedures, Organizing Your Protections, Security Technology, Being Prepared	9
Unit II	**Footprinting and Reconnaissance and Scanning Networks** Open Source Intelligence, Domain Name System, Passive Reconnaissance, Website Intelligence, Technology Intelligence - Scanning Networks - Ping Sweeps, Port Scanning, Vulnerability Scanning, Packet Crafting and Manipulation, Evasion Techniques, Protecting and Detecting	9
Unit III	**Enumeration and System Hacking** Service Enumeration, Remote Procedure Calls, Server Message Block,Simple Network Management Protocol, Simple Mail Transfer Protocol, Web-Based Enumeration - System Hacking - Searching for Exploits, System Compromise, Gathering Passwords , Password Cracking, Client-Side Vulnerabilities, Living Off the Land, Fuzzing , Post Exploitation	9
Unit IV	**Malware and Sniffing** Malware Types, Malware Analysis, Creating Malware, Malware Infrastructure, Antivirus Solutions , Persistence - Sniffing - Packet Capture, Packet Analysis , Spoofing Attacks	9
Unit V	**Social Engineering** Social Engineering, Physical Social Engineering,Phishing Attacks , Website Attacks, Wireless Social Engineering , Automating Social Engineering - Attack and Defense - Web Application Attacks, Denial-of-Service Attacks, Application Exploitation	9
Practical Component		
Exercises	Perform the following using appropriate tools:	30

	1. Reconnaissance - using websites and at least 3 reconnaissance tools 2. Network Scanning 3. Port Scanning 4. Vulnerability Scanning 5. All possible enumerations 6. Password Cracking - Hashcat and John the Ripper 7. Creating Malware 8. Hacking 9. Privilege Escalation 10. SQL Injection	
Recommended Learning Resources		
Print Resources	1. Ric Messier, " CEH v11 Certified Ethical Hacker Study Guide" , John Wiley, 2021. 2. Daniel Graham, " Ethical Hacking- A Hands on Introduction to Breaking In ", No Starch Press, 2021.	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

Year	II	Course Code: CSCY204	Credits	3
Sem.	III	Course Title: Server Administration	Hours	60
			Category	B
Course Prerequisites, if any	● Basic knowledge of Enterprise IT Infrastructure			
Internal Assessment Marks: 50	End Semester Marks: 50	Duration of ESA (Practical): 03 hrs.		
Course Outcomes	● Learn the management of system resources and web services ● Understand the Mail Server Administration and Relational Databases ● Learn Virtualization and Containerization Technologies ● Develop knowledge in Streaming, Communication, and Version Control Systems ● Understanding and Implementation of Collaboration Tools and Performance Monitoring			

Unit No	Course Content	Hours
	Theory Component	
Unit I	**Management of System Resources and Web Services** Managing User Groups and Accounts – user account – group account – managing file permissions – getting root privileges – installing and configuring the Apache web server.	6
Unit II	**Mail Server Administration** Working with Mail Servers – IMAP and POP3, email accounts, mail filtering, troubleshooting the mail server – Zimbra mail server – installing relational databases with MySQL, storing and retrieving, exporting and importing data, user management.	6
Unit III	**Virtualization and Containerization Technologies** Creating Virtual Machine with KVM – Managing Virtual Machines – Openstack – Installing, Starting, and Managing Docker Containers – Dockerfile – Docker Volumes – Monitoring and Securing Docker Containers.	6
Unit IV	**Streaming and Communication** Streaming with Ampache – installing – uploading contents – on-the-fly transcoding – API access for remote streaming – streaming music with Ampache – Communications Server with XMPP – Installing Ejabberd – Creating users and connecting with XMPP Client – Ejabberd installation.	6
Unit V	**Collaboration Tools** Enabling group chat – Chat server with Node JS – Git Hosting – Creating and Managing Git Contents – GitLab server – Collaboration Tools – VNC – Hackpad – collaborating document editor – Mattermost.	6
	Practical Component	
Exercises	1. Creating users and user group accounts with required access permissions 2. Installing and Configuring Apache web server Tomcat web server 3. Installing and Configuring mail servers with IMAP and POP3	30

	4. Installing and Configuring MySQL server 5. Installing and Configuring KVM (Kernel-based Virtual Machine) 6. Installing and Configuring Openstack and Docker Containers 7. Installing and Configuring Apache 8. Installing and Configuring Ejabberd 9. Creating and Managing GIT contents 10. Installing and Configuring collaboration tools-VNC-Hackpad-Mattermost Open Source used : Apache webserver, Tomcat, IMAP, Ejabberd, VNC, MySQL, POP3.	
Recommended Learning Resources		
Print Resources	1. Uday R. Sawant, Oliver Pelz, Jonathan Hobson, William Leemans, "Linux: Powerful Server Administration", Packt Publishing, 2017. 2. Vishal Rai, "Expert Linux Administration Guide", BPB Publications, 2022.	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

Year	II	Course Code: CSCY205	Credits	3
Sem.	III		Hours	60
		Course Title : Black Hat Python	Category	B

Course Prerequisites, if any	● Knowledge of Python Programming, Network Essentials, Fundamentals of Cybersecurity, Ethical Hacking	
Formative Assessment Marks: 50	Summative Assessment Marks: 50	Duration of ESA (Practical) : 03 hrs.
Course Outcomes	● Understanding the basic concepts of performing hacking using Python programming ● Learning about the python packages for performing hacking ● Being able to comprehend various hacking techniques in Python programming ● Being able to perform various hacking tasks using Python Programming ● Learn to develop custom Python codes for required hacking tasks	

Unit No.	Course Content	Hours
Unit I	**Basic Networking Tools and Writing a Sniffer** Writing TCP Client, UDP Client, TCP Server, Replacing Netcat with Python code, Building a TCP Proxy, SSH with Paramiko, SSH Tunneling – Building a UDP Host Discovery Tool, Packet Sniffing with on Windows and Linux, Decoding the IP Layer, Decoding ICMP.	**9**
Unit II	**Owning the Network with SCAPY and Web Hackery** Stealing Email Credentials, ARP Cache Poisoning, pcap processing – Using Web Libraries, Mapping Open Source Web App Installations, Brute Forcing Directories and File Locations, Brute Forcing HTML Form Authentication	**9**
Unit III	**Extending BURP Proxy and Github Command and Control** Burp Fuzzing, Using Bing for Burp, Turning Website Content into Password Gold – Creating GitHub Modules, Configuring the Trojan, Building a GitHub aware Trojan	**9**
Unit IV	**Common Trojaning Tasks on Windows and Exfiltration** Keylogging, Taking Screenshots, Pythonic Shellcode Execution, Sandbox Detection - Encrypting and Decrypting Files, Email Exfiltration, File Transfer Exfiltration, Exfiltration via a Web Server	**9**
Unit V	**Windows Privilege Escalation and Offensive Forensics** Creating the vulnerable Black Hat Service, Creating a Process Monitor, Windows Token Privileges, Winning the race, Code Injection – General Reconnaissance, User Reconnaissance, Vulnerability Reconnaissance, Volshell Interface, Custom Volatility Plug-Ins	**9**
Practical Component		
	Write python programs for the following: 1. Basic network programs involving client, and server 2. Performing host discovery 3. Creating SSH with python 4. Packet sniffing 5. ARP cache poisoning 6. Brute forcing directories and file locations	

	7. Brute forcing HTML form authentication 8. Keylogging of a target system 9. Taking screenshots of a target system 10. Encrypting and decrypting files Open source used : Python	
Recommended Learning Resources		
Print Resources	1. Justin Seitz and Tim Arnold,Black Hat Python, Python Programming for Hackers and Pentesters, No Starch Press, 2021. 2. Akram Press, Python Programming for Ethical Hacking 2: Use Python as a Programming Language to explore various Ethical Hacking Techniques and Tools, Kindle Edition, 2023. 3. Furqan Khan, 2019, Hands-On Penetration Testing with Python: Enhance your Ethical Hacking Skills to Build Automated and Intelligent Systems, Packt Publishing, Kindle Edition.	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

SEMESTER IV

Year	II	Course Code: CSCY206	Credits	4
Sem.	IV	Course Title: Computer System Architecture	Hours	75
			Category	C
Course Prerequisites, if any	● Basic knowledge of Computer and Digital Logic			
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory): 03 hrs. Duration of ESA (Practical): 03 hrs.		
Course Outcomes	● Understand the concept of digital electronics and logic circuits ● Working with binary and arithmetic operations ● Understand the organization of CPU and working principles ● Understand the Input-Output organization in a computer ● Understand the Memory organization in a computer			

Unit No.	Course Content	Hours
	Theory Component	
Unit I	**Digital Logic Circuits** Digital Computers - Logic Gates - Boolean Algebra - Map Simplification - Combinational - Circuits - Flip-Flops - Sequential Circuits - Digital Components	9
Unit II	**Data Representation and Transfer** Datatypes - Complements - Fixed - Point Representation - Floating Point Representation - Register Transfer - Bus and Memory Transfer - Arithmetic - Logic and Shift Microoperations	9
Unit III	**CPU Organization** Register and Stack - Instruction Format - Addressing Modes - Data Transfer and Manipulation - Program Control - RISC - Basics of Pipelining	9
Unit IV	**Input-Output Organization** Peripheral devices - I/O Interface - Asynchronous data transfer - Modes of transfer - Priority Interrupt - DMA - Serial Communication	9
Unit V	**Memory Organization** Memory Hierarchy - Main Memory - Auxiliary Memory - Associative Memory - Cache Memory - Virtual Memory - Memory Management Hardware	9
	Practical Component	
List of Exercises	1. Simplify Boolean expressions using Karnaugh maps. 2. Design a combinational circuit 3. Implementing Logical Left and Right Shifts 4. Understand different data types and how to calculate complements 5. Evaluate performance improvement through instruction level parallelism 6. Analyze the effect of cache performance on system performance 7. Understand the impact of memory hierarchy on access time	30
	Recommended Learning Resources	
Print Resources	1. Morris Mano, “Computer System Architecture”, Pearson Education, 2017.	
Syllabus Design: Dr. Sukhvinder Singh, Assistant Professor, PUDoCS		

Year	II	Course Code: CSCY207	Credits	4
Sem.	IV	Course Title: Design and Analysis of Algorithms	Hours	75
			Category	C
Course Prerequisites, if any	● Basic Knowledge of Data Structures and Programming.			
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory): 03 hrs. Duration of ESA (Practical): 03 hrs.		
Course Outcomes	● Analyze the efficiency of algorithms and compare their performance using appropriate metrics ● Understand the general approach of Brute Force and Divide and Conquer algorithms ● Understand the principles of the Greedy Method in algorithm design ● Understand the principles of Dynamic Programming ● Understand the principles of Backtracking and branch and bound strategies in algorithm design			

Unit No.	Course Content	Hours
	Theory Component	
Unit I	**Introduction** Notation of Algorithm - Analysis of Algorithm Efficiency - Asymptotic Notations and Basic Efficiency classes - Mathematical Analysis of Non-Recursive and recursive Algorithms	9
Unit II	**Divide and Conquer** Brute Force and Divide and conquer - Binary Search – Finding the maximum and minimum – merge sort - quick sort-	9
Unit III	**Greedy Method** General method - Knapsack problem - Job Sequencing - Spanning Trees - Prims's Algorithm and Kruskal's Algorithm	9
Unit IV	**Dynamic Programming** General method - Principle of Optimality - Multistage Graphs - 0/1 Knapsack - Travelling Salesman Problem-	9
Unit V	**Backtracking & Branch Bound** Backtracking-General Method – 8 Queen Problem - Sum of Subsets - Hamiltonian Cycles- Branch and Bound: Introduction FIFO Solution – LC Branch and Bound – 0/1 Knapsack	9
	Practical Component	
Exercises	1. Write recursive and iterative algorithms and analyze their time complexities using Big-O notation 2. Implement and compare the efficiency of sorting algorithms (e.g., bubble sort, quicksort) on different input sizes 3. Implement merge sort and analyze its time complexity with different input sizes 4. Implement a greedy algorithm for the knapsack problem and analyze its efficiency 5. Implement Prim's algorithm for finding the minimum cost spanning tree 6. Implement Kruskal's algorithm for the same purpose and compare the results	30

	7. Solve the 0/1 knapsack problem using dynamic programming and analyze the time complexity 8. Implement a backtracking solution for the subset sum problem and analyze its efficiency	
Recommended Learning Resources		
Print Resources	1. Horowitz, E. and Sahani, S, "Fundamentals of Computer Algorithms", Universities press, Second Edition, 2008. 2. S.Sridar, "Design and Analysis of Algorithms", Oxford University Press, 2014.	
Syllabus Design: Dr. T. Vengattaraman, Associate Professor, PUDoCS		

Year	II	**Course Code: CSCY208** **Course Title: Database Management Systems**	**Credits**	4
			Hours	75
Sem.	IV		**Category**	**C**
Course Prerequisites, if any	● Knowledge of data structures, programming and file-handling			
Internal Assessment Marks: 25	End Semester Marks: 75		Duration of ESA (Theory): 03 hrs. Duration of ESA (Practical): 03 hrs.	
Course Outcomes	● Understand the fundamentals of relational Model ● Design real time applications using database query language (SQL) ● Familiarize with the different kinds of PL/SQL objects ● Understand the various database applications using the Relational model, ER model and EER model ● Construct and normalize conceptual data models			

Unit No.	**Course Content**	**Hours**
	Theory Component	
Unit I	**Introduction to Relational model** Structure of relational database, Database schema, Keys, Schema diagram, Relational Query language, Relational Algebra.	9
Unit II	**Introduction to SQL** SQL data definition, basic structure of SQL Queries, set operations, null values, aggregate functions, nested subqueries	9
Unit III	**Intermediate and advanced SQL** Join expressions, views, transaction, integrity constraints, functions and procedures, triggers.	9
Unit IV	**Database design using ER model** The Entity-Relationship model, complex attributes, mapping cardinalities, primary key, removing redundant attributes in entity sets, reducing ER diagrams to relational schemas, extended ER features.	9
Unit V	**Relational database design** Decomposition using functional dependencies, normal forms, functional dependency theory, algorithms for decomposition using functional dependencies, decomposition using multivalued dependencies.	9
	Practical Component	

Exercises	1. Implement the DDL commands using SQL 2. Implement the DML commands 3. Implement the DDL constraints, DCL, and TCL commands 4. Implement various built functions and aggregate functions 5. Implement the various join operations 6. Implement the various nested subqueries 7. Creation and manipulation of Views 8. Practice the basics of PL/SQL [control structures] 9. Create the functions and procedures using PL/SQL 10. Create the Triggers using PL/SQL	30
Recommended Learning Resources		
Print Resources	1. Abraham Silberschatz, Henry F. Korth and S.Sundarshan, "Database System Concepts ", Seventh Edition, McGraw Hill International Edition, 2021. 2. Brumm.B, "Beginning Oracle SQL for Oracle Database 18c: From Novice to Professional", First Edition**,** Apress, 2019. 3. Kevin Loney, Bob Bryla , "Oracle Database 12c The Complete Reference", First Edition, McGraw Hill, 2013.	
Syllabus design : Dr. T.Chithralekha, Professor, PUDoCS Dr.S.L.Jayalakshmi, Assistant Professor, PUDoCS		

Year	II	Course Code: CSCY209	Credits	4
Sem.	IV		Hours	75
		Course Title: Fundamentals of Cryptography	Category	C

Course Prerequisites, if any	● Basic knowledge of computer, networks and internet	
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory) : 03 hrs. Duration of ESA (Practical) : 03 hrs.
Course Outcomes	● Understand the basics of cryptography ● Learn the various cryptographic algorithms and implement them ● Understand the working of financial cryptography ● Familiarize with the various cryptographic protocols ● Understand network and the operating system security	

Unit No.	Course Content	Hours
	Theory Component	
Unit I	**Introduction to Cryptography** History and overview of Cryptography – Introduction to Secure Programming - API's for Secure Programming - Java Cryptography Extension – .Net Cryptography Extension - Foundation of Computer and Information Security: Definition and its needs, Triad and Parkerian Hexad security models and issues- Attacks and its types – Threats, vulnerabilities and Risk - Risk management	9
Unit II	**Modern Cryptography** Symmetric Key Encryption - Message Integrity – Public Key Cryptography – Digital Signatures – Implementation of DES, RSA, TDES, ECC, IDEA, MD, SHA – Implementing all the algorithms using JCE/. NCE	9
Unit III	**Financial Cryptography** Cryptocurrency - Block chain Applications – Contactless Payments and Ticketing Systems – Digital Cash and Payment Systems – Secure banking and Financial Services – Microfinance and Micropayments – Implementation of Cryptocurrency and Block chain using JCE/. NCE	9
Unit IV	**Cryptographic Protocols** SSL/TLS, SSH, TLS, HTTP/HTTPS, IPSEC, P2P, PGP – Security Protocols – Implementation of All Protocols using JCE/. NCE	9
Unit V	**Network and Operating System Security** Human element Security – Gathering information for Social Engineering Attacks and its types, building security awareness – Physical threat Identification and control, Protecting- people, data and equipment – Designing secure network using firewall and IDS – Protecting Network traffic using network security tools – OS hardening – Protecting against Malware – OS security tools for scanning and assessment of vulnerability	9
	Practical Component	
Practical Component:	Write Java / Python programs to implement the following: 1. DES 2. TDES	30

	3. IDEA 4. RSA 5. ECC 6. MD 7. SHA 8. SSL 9. TLS 10. PGP	
Recommended Learning Resources		
Print Resources	1. Jason Andress, Foundations of Information Security - A Straightforward Introduction William Pollock Publisher, 2019. 2. Atul Kahate, Cryptography and Network Security, McGraw Hill Education, 2019. 3. Jonathan Knudsen, Java Cryptography, Kindle Edition, 2023, 4. William Stallings, Cryptography and network security, Pearson Education, 2023.	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

SEMESTER V

Year	III	Course Code: CSCY301	Credits	4
			Hours	75
Sem.	V	Course Title: Operating Systems	Category	C

Course Prerequisites, if any	● Knowledge of computers & computer organization	
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory): 03 hrs Duration of ESA (Practical): 03 hrs
Course Outcomes	● To understand the basic concepts of Operating System and Process ● To learn the various mechanisms of CPU scheduling, process synchronization and deadlocks ● To understand how the memory is utilized ● To analyze various File System methods and Disk scheduling algorithms ● Evaluate system structures in various operating systems, such as Linux and Windows and identifying similarities and differences	

Unit No.	Course Content	Hours
	Theory Component	
Unit I	**Overview and Process management** Introduction: Operating System Structures - Operating systems services - System calls. Process Management**:** Process Concept – process scheduling-operation on processes-Inter process communications- Threads.	9
Unit II	**Scheduling algorithms and Process Synchronization** CPU Scheduling: Basic Concepts – Scheduling Algorithms. Process Synchronization**:** Critical Section problem – Semaphores - Classical problems of synchronization-Monitors. Deadlock: Deadlock Characterization-Deadlock Handling-Deadlock Prevention-Deadlock Avoidance-Deadlock Detection-Deadlock Recovery.	9
Unit III	**Memory Management** Main Memory: Contiguous Memory Allocation-Paging-Structure of the Page Table –Swapping. Virtual Memory: Demand Paging-Page Replacement-Thrashing.	9
Unit IV	**Storage Management** Mass Storage structure: Overview- HDD (Disk) Scheduling – storage management- RAID Structure. File Systems: File concepts – Access methods – Directory Structure – File Protection –File system Implementation- File-System Structure- File-System Operations- Allocation methods.	9
Unit V	**Case Studies** The Linux system: Design principles – kernel modules-process management- Scheduling- Memory Management-Linux File System. Windows Operating system: Systems components- Windows File System.	9
	Practical Component	

Exercises	1. Practice the file handling utilities, Process utilities, Disk utilities, and Networking commands (ipconfig, ping, arp, route, netstat) 2. Write a program to implement various system call operations 3. Write a program to demonstrate various File management operations 4. Write a program to simulate CPU scheduling algorithms: FCFS, SJF, Round Robin, and priority 5. Write a program to simulate Intra & Inter – Process Communication (IPC) techniques: Pipes, Messages Queues, and Shared Memory 6. Write a program to simulate solutions to Classical Process Synchronization Problems: Dining Philosophers, Producer-Consumer, Readers – Writers 7. Write a program to simulate the Bankers Algorithm for Deadlock Avoidance 8. Write a program to simulate Page Replacement Algorithms: FIFO, Optimal, LRU 9. Write a program to simulate the implementation of HDD Scheduling Algorithms: FCFS, SCAN, C-SCAN 10. Case study on Linux and Windows Operating systems features and prepare a report on the same	30
Recommended Learning Resources		
Print Resources	1. Abraham Silberschatz, Peter B Galvin, G. Gagne, "Operating Systems Concepts", 10th Edition, Addison Wesley, 2018. 2. William Stallings, "Operating Systems: Internals and Design Principles", 10th Edition, Prentice Hall, 2021.	
Syllabus design : Dr. T.Chithralekha, Professor, PUDoCS Dr.S.L.Jayalakshmi, Assistant Professor, PUDoCS		

<table>
<tr><td>Year</td><td>III</td><td colspan="2">Course Code: CSCY302</td><td>Credits</td><td>4</td></tr>
<tr><td rowspan="2">Sem.</td><td rowspan="2">V</td><td colspan="2" rowspan="2">Course Title: Mathematical Foundations of Computer Science</td><td>Hours</td><td>75</td></tr>
<tr><td>Category</td><td>A</td></tr>
<tr><td>Course Prerequisites, if any</td><td colspan="5">● Knowledge of functions, algebra, and pre-calculus</td></tr>
<tr><td>Internal Assessment Marks: 25</td><td colspan="2">End Semester Marks: 75</td><td colspan="3">Duration of ESA (Theory): 03 hrs.</td></tr>
<tr><td>Course Outcomes</td><td colspan="5">● Understand logical statement structures
● Apply operations in problem-solving
● Analyze integer representations and congruences
● Understand counting principles
● Evaluate combinatorial solutions</td></tr>
<tr><td>Unit No.</td><td colspan="3">Course Content</td><td colspan="2">Hours</td></tr>
<tr><td colspan="6">Theory Component</td></tr>
<tr><td>Unit I</td><td colspan="3">Logic and Proofs
Propositional Logic – Predicates and Quantifiers – Rules of Inference - Proofs – Methods and Strategy</td><td colspan="2">15</td></tr>
<tr><td>Unit II</td><td colspan="3">Basic Structures
Sets – Functions – Sequences and Summations– Matrices Relations – properties – representation</td><td colspan="2">15</td></tr>
<tr><td>Unit III</td><td colspan="3">Number Theory
Divisibility and Modular Arithmetic – Integer Representations and Algorithms – Primes and Greatest Common Divisors – Congruences</td><td colspan="2">15</td></tr>
<tr><td>Unit IV</td><td colspan="3">Induction and Recursion

Mathematical Induction - Strong Induction and Well Ordering - Recursive Definitions and Structural Induction</td><td colspan="2">15</td></tr>
<tr><td>Unit V</td><td colspan="3">Counting
Basics – Pigeonhole principle – Permutations and Combinations – Binomial Coefficients</td><td colspan="2">15</td></tr>
<tr><td colspan="6">Practical Component</td></tr>
<tr><td></td><td colspan="3">-</td><td colspan="2">-</td></tr>
<tr><td colspan="6">Recommended Learning Resources</td></tr>
<tr><td>Print Resources</td><td colspan="5">1. Kenneth H. Rosen, “Discrete Mathematics and its Applications”, Seventh Edition, McGraw Hill, Seventh Edition, 2017.
2. Trembley. J.P and Manohar. R., “Discrete Mathematical Structures with Applications to Computer Science”, Tata McGraw Hill,, 2020.</td></tr>
<tr><td colspan="6">Syllabus design: Dr. M.Sathya, Assistant Professor, PUDoCS</td></tr>
</table>

Year	III	Course Code: CSCY303	Credits	4
Sem.	V	Course Title: Computer Networks	Hours	75
			Category	C
Course Prerequisites, if any	Fundamentals of computers			
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory): 03 hrs. Duration of ESA (Practical): 03 hrs.		
Course Outcomes	● Learn the basics of Network topology ● Learn about the various physical network media ● Understand the functionalities of all the network layers ● Familiarize the protocols of different layers ● Implement the various network protocols			

Unit No.	Course Content	Hours
	Theory Component	
Unit I	**Introduction** Introduction to Networks, Topology, Network Architecture, Reference Models, Transmission Media-Multiplexing, Switching	9
Unit II	**Data link layer** Design Issues, Error Detection and Correction , Elementary Data, Link Protocols, Sliding window Protocols	9
Unit III	**Network Layer** Design Issues, Routing , Logical Addressing, IP Working- IPV4 Vs IPV6, Address Mapping, delivery, Forwarding and routing	9
Unit IV	**Transport Layer** The Transport Service, Service provided to the Upper Layers, Flow Control & Buffering, TCP Congestion Control, UDP , TCP Vs UDP	9
Unit V	**Application layer** Domain Naming System, DNS Namespace, Resource Records, Name Servers , Electronic mail, Messages Formats, Message Transfer	9
	Practical Component	
Exercises	1. Implementation of Basic Chat 2. Implementation of Multiple User Chat 3. Implementation of File Transmission 4. Implementation of Simple Mailing Application 5. Implementation of Client Server Application 6. Given IP address and subnet mask, Computation of (i)Subnet addresses (ii) Number of hosts in each subnet (iii IP addresses of hosts in each subnet 7. Implementation of Error Detection / Error Correction Techniques 8. Implementation of socket program Remote Procedure Call	30

	9. Implementation of any 1 routing protocol 10. Implementation of congestion control protocol	
Recommended Learning Resources		
Print Resources	1. Andrew S. Tanenbaum, David J. Wetherall, “Computer Networks”, Fifth Edition, Prentice Hall publisher, 2022. 2. Larry L. Peterson, Bruce S. Davie, “Computer Networks: A Systems Approach”, Fifth Edition, Morgan Kaufmann Publishers Inc., 2015. 3. James F. Kurose, Keith W. Ross,” Computer Networking - A Top-Down Approach Featuring the Internet”, Seventh Edition, Pearson Education, 2022.	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

Year	III	Course Code: CSCY304	Credits	4
Sem.	VI	Course Title: Network Security	Hours	75
			Category	C
Course Prerequisites, if any	● Basic Knowledge of computer networks			
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory): 03 hrs. Duration of ESA (Practical): 03 hrs.		
Outcomes	● Learn about the basic network security threats, vulnerabilities and attacks ● Understand the use of encryption, digital signatures, digital certificates, Kerberos authentication systems for network security ● Learn about www and email security ● Understand Operating System, LAN and Router security ● Applying the network security principles to design secure networks			

Unit No.	Course Content	Hours
	Theory Component	
Unit I	**Basic Security Concepts** Background , History, The Security Trinity, Information Security, Risk Assessment, Security Models, Basic Terminology - Threats, Vulnerabilities, and Attack - Protocols, The OSI Reference Model, TCP/IP Protocol Suite, Threats Vulnerabilities and Attacks, Useful Websites, Search Engines, Mailing List	9
Unit II	**Encryption, Digital Signatures and Certificate Authorities, - Kerbero**s Overview, Stream Ciphers, Block Ciphers, Breaking Ciphers, Encryption, Public Key Cryptosystems, Message Integrity, Authentication, Digital Signatures, Digital Certificate, Certificate Authorities, Public Key Infrastructure, Kerberos Key Exchange - Kerberos, Kerberos' Limitations	9
Unit III	**WWW and E - mail Security** Encryption on the World Wide Web - The World Wide Web (WWW), Secure Sockets Layer , Secure HTTP (SHTTP), Microsoft's Internet Explorer, Netscape Navigator, Authenticode Certificates - E-Mail - E-Mail Issues, E-Mail Security, Secure E-Mail Protocols, Web-Based E-Mail Services, Security of Stored Messages, Identity: Spoofing and Hiding , E-Mail as a Weapon, Policies, E-Mail Privacy	9
Unit IV	**Operating System and LAN Security** Operating System Guidelines, Passwords, Password Guidelines, Access Control, Permissions , General Recommendations, Modems, Information Availability, Useful Tools - LAN Security - LAN Guidelines, Controlling End User Access, Concurrent Logins, Available Disk Space, Restrictions to Location or Workstation, Access to Directories and Trustee Rights, Remove Inactive Accounts, Single Sign-On,	9

	Segmenting LAN Traffic, Honeypot Systems, Static IP Addresses Versus Dynamic Host Configuration Protocol	
Unit V	**Media and Protocols , Routers Security** Network Media, Wireless LAN, Wireless WAN , Dedicated Lease Lines, Packet-Switched Networks, Frame Relay, Asynchronous Transfer Mode, Cable Television,x Digital Subscriber Line (xDSL), The Internet- Routers and SNMP - Router Issues , Risks ,Cisco IOS, Cisco Secure Integrated Software, Simple Network Management Protocol (SNMP)	9
Practical Component		
Exercises	1. Performing a study of the various network security attacks and preparing a report on the same 2. Using Open SSL perform the following a. Symmetric Key encryption b. Asymmetric Key encryption c. Digital Signatures d. Creating Digital Certificates e. SSL f. Email Security 3. Study the security features of Windows and Linux Operating Systems and demonstrate the use of the same using appropriate settings and configurations 4. Configuring security using SNMP protocol 5. Configure SNORT tool to capture network traffic and create custom rules to detect and alert on specific types of network traffic viz pings, port scans, etc.	30
Recommended Learning Resources		
Print Resources	1. John E. Canavan,Fundamentals of Network Security,Artech House, 2017 2. Pravir Chandra, Matt Messier, John Viega, Network Security with Open SSL, O'Reilly, 2002. 3. William Stallings, Cryptography and Network Security, Seventh Edition, Pearson Education, 2017	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

SEMESTER VI

<table>
<tr><td rowspan="2">Year</td><td rowspan="2">III</td><td colspan="2" rowspan="2">Course Code: CSCY306

Course Title: Management Strategies and Concepts</td><td>Credits</td><td>4</td></tr>
<tr><td>Hours</td><td>75</td></tr>
<tr><td>Sem.</td><td>VI</td><td>Category</td><td>A</td></tr>
<tr><td>Course Prerequisites, if any</td><td colspan="5">● Basic knowledge of an organization and its functioning</td></tr>
<tr><td>Internal Assessment Marks: 25</td><td colspan="2">End Semester Marks: 75</td><td colspan="3">Duration of ESA (Theory): 03 hrs.</td></tr>
<tr><td>Course Outcomes</td><td colspan="5">● Understand the fundamentals of Management Theories
● Learn the management & communication Process Concepts
● Analyse the performance of decentralized and centralized organizational structures
● Analyse the different leadership styles and their effects on team performance and organizational culture
● Evaluate the effectiveness of the strategies in enhancing productivity and efficiency</td></tr>
<tr><td>Unit No.</td><td colspan="4">Course Content</td><td>Hours</td></tr>
<tr><td colspan="6">Theory Component</td></tr>
<tr><td>Unit I</td><td colspan="4">Management Theories
Science Theory and Practice - Management and Society: Social Responsibility and Ethics. The nature and purpose of planning - objectives – Strategies Policies and planning premises.</td><td>15</td></tr>
<tr><td>Unit II</td><td colspan="4">Decision Making
Process of decision making- organizing- Nature and purpose of organizing – Basics of departmentalization - Line/Staff Authority and Decentralization - Effective Organizing and organizational structure & culture.</td><td>15</td></tr>
<tr><td>Unit III</td><td colspan="4">Human Resource Management & Selection
Staffing-Manpower planning - Recruitment & Selection-Performance appraisal and career strategy - Organizational development.</td><td>15</td></tr>
<tr><td>Unit IV</td><td colspan="4">Managing the Human factor
Motivation - Leadership – Communication</td><td>15</td></tr>
<tr><td>Unit V</td><td colspan="4">The System & Process of Controlling
Control techniques and Information Technology - Productivity and Operations Management - Overall and Preventive Control - Towards a Unified - Global management theory.</td><td>15</td></tr>
<tr><td colspan="6">Recommended Learning Resources</td></tr>
<tr><td>Print Resources</td><td colspan="5">1. Herald Knootz and Heinz Weihrich, “Essentials of Management”, Eleventh edition, McGraw-Hill Publishing Company, 2020.
2. Fred R. David and Forest R. David, "Strategic Management: Concepts and Cases", Prentice Hall India Learning Private Limited, Sixteenth Edition, 2020.</td></tr>
<tr><td colspan="6">Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS
Dr. S.L.Jayalakshmi, Assistant Professor, PUDoCS</td></tr>
</table>

Year	III	Course Code: CSCY307	Credits	4
Sem.	VI	Course Title: Software Engineering Theory and Practice	Hours	75
			Category	C
Course Prerequisites, if any	● Basic knowledge of programming and information systems			
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory): 03 hrs. Duration of ESA (Practical): 03 hrs.		
Course Outcomes	• Understand the fundamental concepts of design thinking • Analyze and document the software requirements • Apply appropriate software engineering design concepts to develop software. • Apply software testing strategies • Understand and consider the significance of security in software development process			

Unit No.	Course Content	Hours
	Theory Component	
Unit I	**Introduction to Design Thinking** Design process - Traditional design - Design thinking - Existing sample design projects - Study on designs around us - Compositions/structure of a design - Innovative design - Breaking of patterns - Reframe existing design problems - Principles of creativity Empathy - Customer Needs - Insight-leaving from the lives of others/standing on the shoes of others - Observation.	9
Unit II	**Software Engineering and Software Requirements** Defining software engineering, Software life cycle models, Selection of a life cycle model - Requirements engineering, Types of requirements, Feasibility studies, Requirements elicitation, Requirement analysis, Requirement documentation, Requirement validation.	9
Unit III	**Software Project Planning** Size estimation, Cost estimation, Models, Constructive cost model, Software risk management, Software design, Modularity, Strategy of design, Function oriented design, Object oriented design.	9
Unit IV	**Testing Strategies** A strategic approach to software testing, Test strategies for conventional software, Black-Box and White-Box testing, Validation testing, System testing, The art of Debugging.	9
Unit V	**Secure Software Engineering** Introduction - The problem – Software assurance and software security – Threats to software security – Software insecurity – Benefits of detecting software security defects early – Managing secure software development – Defining Properties – Influencing the security properties of software – To assert and specify desired security properties.	9
	Practical Component	
Exercises	1. Conceptualize a novel app that will help to save: a) Energy b) Water	30

	c) Food 2. Apply the phases of Software Development Life Cycle for the following applications and develop the same : 1. Library Management System 2. Hospital Management System 3. Design the above two systems with security features and implement the same.	
Recommended Learning Resources		
Print Resources	1. Tim Brown, "Change by Design: How Design Thinking Transforms Organizations and Inspires Innovation", 1st edition, HarperCollins Publishers Ltd, 2019. 2. Roger S. Pressman, Bruce Maxim, "Software Engineering, A Practitioner's Approach", 9th edition, McGraw Hill International Edition, 2023. 3. Julia H. Allen, "Software Security Engineering : A Guide for Project Managers", 1st edition, 2008.	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

ear	III	**Course Code: CSCY308**	**Credits**	4
Sem.	VI	**Course Title : Distributed Systems**	**Hours**	75
			Category	C
Course Prerequisites, if any	Basic knowledge in Operating Systems and Computer Networks			
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory): 03 hrs. Duration of ESA (Practicals): 03 hrs.		
Course Outcomes	● Learn basic concepts of Distributed Systems· ● Understand state-of-the-art distributed system· ● Design and develop Client/Server Applications ● Setup fault tolerance and replication servers ● Design and implement CORBA and DCOM			

Unit No.	**Course Content**	**Hours**
	Theory Component	
Unit I	**Introduction** Definition – Goals – Hardware and Software Concepts – Client/Server Model Communication – Layered Protocols RPC – Remote Object Invocation – Message Oriented Communication.	9
Unit II	**Client Server** Client Server and Naming Entity- Threads - Client Server – Code Migration – S/W Agents – Naming Entity – Location Mobile Entity.	9
Unit III	**Synchronization** Distributed Transactions- Synchronization – Clock Synchronization – Logical Clocks – Global States – Election Algorithms – Mutual Exclusion – Distributed Transaction - Consistency and Replication– Data Centric Consistency –Fault Tolerance – Distributed Commit – Recovery	9
Unit IV	**Distributed Objects** Distributed Object Database System: CORBA – DCOM – GLOBE.	9
Unit V	**Distributed File System** Introduction- Distributed File System – Distributed Document Base System – WWW – Distributed Coordination Based System – JINI.	9
	Practical Component	

Exercises	1. Perform arithmetic operation using RMI 2. Calculate simple and compound interest using RMI 3. Implementation of ATM using RMI 4. Implementation of Telephone Directory using RMI 5. Implementation of Quiz Server using Servlets 6. Implementation of Online Shopping System using servlets 7. Implementation of Matrimonial System using servlets 8. Implementation of servlet based Airline Reservation System 9. Create a Word Document with text using DCOM and Visual Basic	30
Recommended Learning Resources		
Print Resources	1. Andrew S. Tanenbaum, Maarten van Steer, Distributed Systems Principles and Paradigms, Third edition, Prentice Hall India, 2017. 2.George Couloursis, Jean Dollomore and Tim Kinderberg, Distributed Systems - Concepts and Design, Addison-Wesley, Fifth edition, 2011.	
Syllabus Design: Dr.T.Sivakumar, Assistant Professor, PUDoCS		

<table>
<tr><td>Year</td><td>III</td><td colspan="2">Course Code: CSCY309</td><td>Credits</td><td>4</td></tr>
<tr><td rowspan="2">Sem.</td><td rowspan="2">VI</td><td colspan="2" rowspan="2">Course Title: Operations Research</td><td>Hours</td><td>75</td></tr>
<tr><td>Category</td><td>A</td></tr>
<tr><td>Course Prerequisites, if any</td><td colspan="5">● Basic Mathematical and Problem Solving Skills</td></tr>
<tr><td>Internal Assessment Marks: 25</td><td colspan="2">End Semester Marks: 75</td><td colspan="3">Duration of ESA (Theory): 03 hrs.</td></tr>
<tr><td>Course Outcomes</td><td colspan="5">● Understand and comprehend the basics of Linear Programing Problem (LPP)
● Llearn LPP solving methods and explore duality in LPP
● Solve assignment problem and their variants
● Find the feasible and optimal solutions for transportation problems
● Perform critical path analysis and reviewing of a project</td></tr>
<tr><td>Unit No.</td><td colspan="3">Course Content</td><td colspan="2">Hours</td></tr>
<tr><td colspan="6">Theory Component</td></tr>
<tr><td>Unit I</td><td colspan="3">Introduction
Operation Research – Definition – Characteristics – Techniques – Applications. LPP – Introduction – Applications and components of LPP – Steps in solving LPP.</td><td colspan="2">15</td></tr>
<tr><td>Unit II</td><td colspan="3">LPP
Mathematical formulation – Graphical method – Simplex method – Artificial variables – Big-M method - Two-phase method – Degeneracy and unbound solutions – Duality in LPP – Formulation – Relationship between primal and dual problems.</td><td colspan="2">15</td></tr>
<tr><td>Unit III</td><td colspan="3">Assignment Model
Mathematical formulations - Hungarian Method – Variants of the Assignment problem.</td><td colspan="2">15</td></tr>
<tr><td>Unit IV</td><td colspan="3">Transportation Problem
Mathematical formulation – Finding basic feasible solutions – NWCR, LCM and VAM – Optimal solution – MODI method.</td><td colspan="2">15</td></tr>
<tr><td>Unit V</td><td colspan="3">Network Scheduling
Introduction – Basic components – Logical sequencing – Rules of network construction – Concurrent Activities – Critical Path Analysis -Activity Time and Floats – Project Evaluation and Review Technique (PERT) – Three Time Estimates – Critical Path Analysis of PERT network – Probability of completion of Project.</td><td colspan="2">15</td></tr>
<tr><td colspan="6">Practical Component</td></tr>
<tr><td></td><td colspan="3">-</td><td colspan="2"></td></tr>
<tr><td colspan="6">Recommended Learning Resources</td></tr>
<tr><td>Print Resources</td><td colspan="5">1. Kanti Swarup, P.K. Gupta, Man Mohan, “Operations Research”, 20th Edition, Sultan Chand & Sons, 2023.
2. Taha H.A., “Operations Research: An Introduction”, 10th Edition, Pearson Education, 2019.</td></tr>
<tr><td colspan="6">Syllabus Design: Dr. G. Krishnapriya, Assistant Professor, PUDoCS
Revised by : Dr. M. Nandhini, Professor, PUDoCS</td></tr>
</table>

Year	III	Course Code: CSCY310	Credits	4
Sem.	VI	Course Title: Information Security Management	Hours	75
			Category	A
Course Prerequisites, if any	● Basic knowledge of Computer Networks and cybersecurity			
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory): 03 hrs.		
Course Outcomes	● Understanding the basics of security and risk management ● Comprehending the various aspects of the information security management ● Understanding the various security management controls required for security management ● Applying information security management concepts in a practical scenario ● Learning the various security management standards			

Unit No.	Course Content	Hours
	Theory Component	
Unit I	**Security and Risk Management** Security, Risk, Compliance, Law, Regulations, and Business Continuity-Confidentiality, integrity, and availability concepts - Security governance principles – Compliance - Legal and regulatory issues - Professional ethic - Security policies, standards, procedures and guidelines	9
Unit II	**Asset Security** Protecting Security of Asset-Information and asset classification - Ownership (e.g. data owners, system owners) - Protect privacy - Appropriate retention - Data security controls - Handling requirements (e.g. markings, labels, storage)	9
Unit III	**Security Engineering** Engineering and Management of Security - Security models - Security evaluation models - Security capabilities of information systems - Security architectures, designs, and solution elements vulnerabilities – Web based systems vulnerabilities - Mobile systems vulnerabilities - Embedded devices and cyber physical systems vulnerabilities	9
Unit IV	**Communication and Network Security** Designing and Protecting Network Security - Secure network architecture design (e.g. IP & non - IP protocols, segmentation) - Secure network components - Secure communication channels - Network attacks	9
Unit V	**Identity and Access Management** Controlling Access and Managing Identity - Physical and logical assets control - Identification and authentication of people and devices - Identity as a service (e.g. cloud identity) – Third-party identity services (e.g. on- premise)	9

	- Access control attacks - Identity and access provisioning lifecycle (e.g. provisioning review)	
Practical Component		
Exercises	1.Consider the IT infrastructure of a typical IT organization and perform the following : i. Perform an inventory of IT assets (Assets, owners, label / classification) ii. Identify the vulnerabilities, threats & risk associated with each asset iii. Identify suitable security controls to protect every asset 2.Perform a study on the various information security standard organizations across the world 3. Perform a study on various security management standards and prepare a report on the same 4.Perform a study of various information security risk management standards and prepare a report on the same 5. Perform a study of various Business continuity standards and prepare a report on the same 6. Perform a study of various incident management standards and prepare a report on the same 7. Perform a study of various disaster recovery standards and prepare a report on the same	30
Recommended Learning Resources		
Print Resources	1. James M. Stewart, Ed Tittel, Mike Chapple 'CISSP: Certified Information Systems Security Professional Study Guide', John Wiley&Sons, 2018. 2. Michael E. Whitman, Herbert J. Mattord, 'Management of Information Security, 6th Edition,Cengage Learning,2018	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

Year	III	Course Code: CSCY311	Credits	4
Sem.	VI		Hours	75
		Course Title : IoT & Security	Category	A

Course Prerequisites, if any	● Knowledge of Computer Networks, Cybersecurity and Internet	
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory) : 03 hrs.
Course Outcomes	● Understanding of IoT ● Learning Security Fundamentals of IoT ● Learning to design Secure IoT ● Studying about Secure Development lifecycle ● Understanding Operational Security Lifecycle	

Unit No.	Course Content	Hours
	Theory Component	
Unit I	**Introduction to IoT** Defining cyber-physical systems, Cybersecurity versus IoT security, The IoT of Today-Modernizing the transportation ecosystem, Smart manufacturing, Smart cities spread across the globe, The importance of cross-industry collaboration, The IoT ecosystem	9
Unit II	**Vulnerabilities, Attacks, and Countermeasures** The classic pillars of information assurance, Threats, Vulnerability, Risks, Primer on attacks and countermeasures-Common IoT attack types, Attack trees, Fault (failure) trees and CPS, IoT attacks-Authentication attacks, Distributed Denial of Service (DDoS), Application security attacks, Wireless reconnaissance and mapping, Security protocol attacks	9
Unit III	**Approaches to Secure Development** The Secure Development Life Cycle (SDLC)-Waterfall-Requirements, Design, Implementation, Verification. Spiral, Agile-Security engineering in Agile, DevOps. Handling non-functional requirements-Security	9
Unit IV	**Secure Design of IoT Devices** The challenge of secure IoT development, goals , IoT systems that mitigate automated attack risks, Secure Design of IoT systems- IoT Systems with secure points of integration, IoT systems to protect confidentiality and integrity, IoT systems that are safe, IoT hardware security.	9
Unit V	**Operational Security Life Cycle** Defining your security policies, Defining system roles, configuring gateway and network security, Securing WSN, Ports, protocols, and services, Gateways, Network services, Network segmentation and network access controls, Bootstrapping and securely configuring devices, Setting up threat intelligence and vulnerability tracking	9
	Practical Component	

Practical Component:	1. Perform a study on all IoT security attacks and prepare a report on the same 2. Collect details about the various IoT security attack incidents which have happened in the last 5 years and prepare a report on the same 3. Prepare a report on the IoT security applications 4. Prepare a report on the IoT security best practices 5. Prepare a report on Embedded Security and Firmware security 6. Make a report on the IoT security companies in India and abroad and the IoT security solutions they are developing 7. Make a report on the top 10 IoT security solutions 8. Make a report on the International standards organizations which have provided standards for IoT security 9. Perform a study on the IoT security standards and frameworks and prepare a report on the same 10. Consider any IoT device and provide a secure design for that device	30
Recommended Learning Resources		
Print Resources	1. Russell, B., & van Duren, D. (n.d.). Practical internet of things security: design a security framework for an Internet connected ecosystem , 2018. 2. IoT: Security and Privacy Paradigm (Internet of Everything (IoE)) [1 ed.] by Souvik Pal (editor), Vicente García Díaz (editor), Dac-Nhuong Le (editor) , CRC Press, 2020.	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

SEMESTER VII

Year	IV	**Course Code : CSCY401**	**Credits**	4
Sem.	VII	**Course Title : Web Engineering**	**Hours**	75
			Category	C
Course Prerequisites, if any	● Knowledge of programming			
Internal Assessment Marks : 25	**End Semester Marks :** 75		**Duration of ESA (Theory) :** 03 hrs. **Duration of ESA (Practical) :** 03 hrs	
Course Outcomes	● Understand the process of web publishing ● Acquire skills developing web pages using HTML ● Acquire skills to style the web pages using CSS ● Acquire skills to build server side web components ● Explore the mobile web development process			
Unit No.	**Course Component**		**Hours**	
Theory Component				
Unit I	**Introduction to World Wide Web** Introduction to web publishing - Web browsers - Web servers - Uniform Resource Locators - Using browser based developer tools.		9	
Unit II	**Introduction to HTML and CSS** Structuring a web page with HTML - Basic elements - Lists - Links - Tables - Images - Forms. Using CSS to style a site - CSS for positioning - Integrating Multimedia elements.		9	
Unit III	**Introduction to JavaScript** The structure - Operators - Variables - Control structures - Functions - Arrays - Objects - Validation.		9	
Unit IV	**Introduction to PHP** Setting up the server - PHP language basics - built-in functions - library functions - using includes - database connectivity - sending email - cookies and sessions-File uploads.		9	
Unit V	**Mobile Web** Mobile browsing needs - text on mobile web - design and page layout - links - images and multimedia - CSS for mobile - making use mobile features - Best practices.		9	
Practical Component				
	1. Build your resume using simple static html 2. Enrich your resume with CSS			

Exercises	3. Implement an HTML Form with javascript validation 4. Build a web application to demonstrate event handling in JavaScript 5. Add a server side component to the task #3 6. Build a server side data storage web application 7. Build a web application to demonstrate session handling 8. Build a web application to demonstrate cookies handling 9. Implement mobile web application 10. Implement file uploads in a web application	30
Recommended Learning Resource		
Print Resources	1. Laura Lemay, Rafe Coburn, Jennifer Kyrnin, "Sams Teach yourself HTML, CSS & Javascript Web Publishing", Pearson Education 2016.	
Syllabus design: Dr.K.S.Kuppusamy, Associate Professor, PUDoCS		

Year	IV	Course Code: CSCY402	Credits	4
			Hours	75
Sem.	VII	Course Title: System Modeling and Simulation	Category	C
Course Prerequisites, if any	● Knowledge of computers, mathematics and programming			
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory): 03 hrs. Duration of ESA (Practical): 03 hrs.		
Course Outcomes	● Understand the fundamentals of modeling and simulation ● Learn about statistical models and input modeling ● Understand the techniques for random number generation ● Perform the simulation of dynamic systems ● Verify the simulation models			

Unit No.	Course Content	Hours
Unit I	**Introduction** Simulation tool - Advantages and disadvantages of Simulation - Areas of application- Systems and system environment - Components of a system- Discrete and continuous systems - Model of a system- Types of Models - DESS Simulation example - Simulation of queuing systems - General Principles.	9
Unit II	**Statistical Models in Simulation** Review of terminology and concepts - Useful statistical models - Discrete distributions - Continuous distributions - Poisson process - Empirical distributions - General Principles - Characteristics of queuing systems - Queuing notation - Long-run measures of performance of queuing systems - Steady-state behavior of M/G/1 queue - Networks of queues.	9
Unit III	**Random-Number Generation** Properties of random numbers - Generation of pseudo-random numbers - Techniques for generating random numbers - Tests for Random Numbers - Inverse transform technique Acceptance -Rejection technique.	9
Unit IV	**Input Modeling** Data Collection - Identifying the distribution with data - Parameter estimation - Goodness of Fit Tests - Fitting a non-stationary Poisson process - Selecting input models without data – Multivariate & Time - Series input models -Types of simulations with respect to output analysis - Stochastic nature of output data - Measures of performance and their estimation	9
Unit V	**Simulation Models** Measures of performance and their estimation - Output analysis for terminating simulations - Output analysis for steady state simulations- Verification, Calibration And Validation - Optimization, Model building, verification and validation - Verification of simulation models - Calibration and validation of models, Optimization via Simulation.	9

Practical Component		
Exercises	1. Simulation of Random Numbers generation 2. Implement Chi-square goodness-of-fit test 3. Implement One-sample Kolmogorov-Smirnov test 4. Implement Test for Standard Normal Distribution 5. Implement Monte-Carlo Simulation 6. Simulation of Single Server Queuing System 7. Simulation of Two-Server Queuing System 8. Simulate and control a conveyor belt system 9. Implement Two-sample Kolmogorov-Smirnov test	30
Recommended Learning Resources		
Print Resources	1. Jerry Banks, John S. Carson II, Barry L. Nelson, David M. Nicol, "Discrete-Event System Simulation", 5th Edition, Pearson Education, 2013. 2. Lawrence M. Leemis, Stephen K. Park " Discrete – Event Simulation: A First Course", Pearson Education, 2013.	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

Year	IV	Course Code: CSCY403 Course Title : Wireless Communication Networks	Credits	4
Sem.	VII		Hours	75
			Category	C
Course Prerequisites, if any	● Knowledge of computer networks			
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory): 03 hrs. Duration of ESA (Practicals): 03 hrs.		
Course Outcomes	● Understand basics of Wireless Communication Networks ● Understand the Satellite Communications concepts and compare the various generations of wireless communications ● Explore the IEEE 802.11 WLAN standard ● Explore WAP and its application ● Understand Wireless LAN Technologies			
Unit No.	**Course Content**		**Hours**	
Theory Component				
Unit I	**Introduction** Wireless Communication Technology- Antennas and Propagation-Antennas, Propagation Modes, Fading in the Mobile Environment. Signal Encoding Techniques- Signal Encoding Criteria, Digital Data-Analog Signals, Analog Data-Analog Signals, Analog Data-Digital Signals.		9	
Unit II	**Satellite Communications** Wireless Networking - Satellite Communications- Satellite Parameters and Configurations, Capacity Allocation-Frequency Division, Capacity Allocation-Time Division Cellular Wireless Networks- Principles of Cellular Networks, First-Generation Analog, Second-Generation - TDMA, CDMA, 3G Systems.		9	
Unit III	**Wireless Lan Standards** Evolution of IEEE 802.11- Introduction to IEEE 802.11 -General Description- Medium Access Control (MAC) for the IEEE 802.11 - WLANs Physical Layer for IEEE 802.11 -WLANs; Radio Systems -IR Systems Applications.		9	
Unit IV	**Mobile IP** Introduction, operation of Mobile IP, Mobile IP terminologies, Wireless Access Protocols: Introduction, Architecture overview, Wireless application environment.		9	

Unit V	**Wireless LAN Technology** Wireless LAN- application, requirements, Technology: Infrared, spread spectrum, Narrowband microwave (radio), Introduction Bluetooth Technologies (Only Overview).	9
Practical Component		
Exercises	1. Study about different Wireless devices like Wi-Fi Dongler, Wireless Access Point, Antenna, Wi-Fi Router 2. Simulate BlueTooth Communication after pairing 3. Simulate a scenario for MANET in NS2 4. Study and analyse the performance of AODV routing protocol using NS2 5. Study and analyse the performance of DSR routing protocol using NS 6. Study and analyse the performance of ZRP routing protocol using NS2	30
Recommended Learning Resources		
Print Resources	1. William Stallings, "Wireless Communications and Networks" 2nd edition, Pearson Prentice Hall, 2008.	
Syllabus Design: Dr.T.Sivakumar, Assistant Professor, PUDoCS		

Year	IV	Course Code: CSCY404	Credits	4
Sem.	VII	Course Title: Digital Forensics	Hours	75
			Category	C
Course Prerequisites, if any	Knowledge of cybersecurity, cyber attacks and cyber crimes			
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory): 03 hrs. Duration of ESA (Practical): 03 hrs.		
Course Outcomes	● Understanding the basics of digital forensics ● Learning to use the digital forensic tools ● Able to perform digital forensics on windows, emails, browsers, social media, mobile phones etc. ● Being able to prepare a forensics analysis report ● Performing digital forensics on real time use cases			
Unit No.	**Course Content**		**Hours**	
Theory Component				
Unit I	**Introduction to Digital forensics and Essential Technical Concepts** Defining digital forensics and goals,Defining cybercrime and cybercrime sources, Computers in cybercrimes, Digital forensics categories, Forensic data analysis, Digital forensic users, Investigation types, Forensics readiness, Digital evidence types, Electronic evidence location, Chain of custody, Examination process- Different number system, Encoding schema, File carving and structure, File metadata, Hash analysis, System memory, Storage, Filesystem, Cloud computing, Windows OS, Networking.		9	
Unit II	**Hard Disks and File Systems and Requirements for a Computer Forensics Lab** File systems, Hard disk, Hard disk forensics, Analyzing the registry files- Digital Forensic Lab, Physical requirements, Environment controls, Digital Forensic equipment, Office electrical equipment, Networked devices.		9	
Unit III	**Acquiring Digital Evidence and Analysis of Digital Evidence** Advanced forensic format, Live memory acquisition, Virtual memory: Swap space, Administration privilege, acquiring non volatile memory, Hard disk acquistion, Acquiring physical resources, Network acquisition- Arsenal Image Mounter, OSFMount, Autopsy, Fireeye tools, Volatility.		9	
Unit IV	**Windows Forensic Analysis and Web Browser and E-mail Forensics** Timeline analysis tools, Data carving, Windows registry analysis, USB device forensics, Printer registry information, File format identification, Windows thumbnail forensics, Windows 10 forensics, Notification area database, Cortana forensics - Web Browser and E-		9	

	mail Forensics - Web Browser Forensics, Google Chrome Browser Forensics, Mozilla Firefox Browser Forensics,Other Browser Forensics tools	
Unit V	**E-mail Forensics and Anti-Forensics Techniques and Report Writing** E-mails around us, E-mail communication steps, E-mail protocols, Examine email headers, Determine sender's , geolocation and time zone - Anti-Forensics Techniques and Report Writing - Anti-forensics, Digital Steganography, Text Steganography, Image Steganography, Audio-video Steganography, Network Steganography, Metadata manipulation, Encryption techniques, Anonymity techniques, Report writing	9
Practical Component		
Exercises	1. Perform disk imaging and analysis FTK tool 2. Perform memory forensics 3. Perform malware analysis 4. Perform steganography 5. Recover deleted files using autopsy 6. Find cybercrime evidence in disk images using the Autopsy tool 7. Perform windows registry and prefetch file analysis for capturing evidence 8. Perform browser forensics 9. Extract exif data from graphic files 10. Prepare a digital forensics report based on the evidence collected for a cybercrime	30
Recommended Learning Resources		
Print Resources	1. Akashdeep Bhardwaj and Keshav Kaushik, " Practical Digital Forensics", BPB Online, 2023 2. Richard Bodinggton, " Practical Digital Forensics", Packt Publishing, 2016. 3. Greg Gogolin, "Digital Forensics Explained", Second Edition, CRC Press, 2021.	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

Year	IV	Course Code: CSCY405	Credits	4
Sem.	VII	Course Title: Security Information and Event Management (SIEM)	Hours	75
			Category	A
Course Prerequisites, if any	● Knowledge of Cybersecurity and Computer Networks			
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory): 03 hrs.		
Course Outcomes	● Understand the basics of SIEM ● Learn how SIEM helps in Infrastructure monitoring and Event Management ● Comprehend how SIEM helps in Incident Management ● Familiarizing with the various SIEM tools ● Understanding how SIEM is being used for managing security in various organizations			
Unit No.	**Course Content**		**Hours**	
Theory Component				
Unit I	**Introduction :** Business Models - IT Business Models, Overview of CIA, Government, Commercial Entities, Universities - Threat Models - The Bad Things That Could Happen, Recognizing Attacks on the IT Systems - Regulatory Compliance - Compliance Regulations, Recommended Best Practices, Prudent Security		9	
Unit II	**SIEM Concepts** Components for Small and Medium size Businesses - The Homegrown SIEM, Log Management Event Correlation, Endpoint Security, IT Regulatory Compliance, Implementation Methodology, Tools Reference - The Anatomy of a SIEM - Source Device, Log Collection, Parsing/Normalization of Logs , Rule Engine/Correlation Engine , Log Storage, Monitoring		9	
Unit III	**Incident Response and Business Intelligence using SIEM** Incident Response - an Incident Response Program, Build an Incident Response Program, Security Incidents and a Guide to Incident Response, Automated Response - Using SIEM for Business Intelligence - Business Intelligence , Common Business Intelligence, Developing Business Intelligence Strategies Using SIEM		9	
Unit IV	**SIEM Tools** AlienVault OSSIM Implementation - Background, Design, Implementation, Web Console - AlienVault OSSIM Operation - Interface, Analysis of a Basic Attack, Analysis of a Sophisticated Attack		9	
Unit V	**Cisco Security: MARS Implementation** Introduction to MARS - Topology, Sessions, and Incidents, Scaling a MARS Deployment - Analyze Requirements - Objectives , Unique Threat Concerns , Infrastructure Inventory		9	
Practical Component				
Exercises	1. Prepare a report on the various SIEM tools available		30	

	and perform a comparison of the same 2. Prepare a report on the various SIEM solutions providing companies in India and abroad and prepare a report on the same 3. Make a report on the various SIEM architectures and their respective components 4. Perform a study on NIST SIEM requirements and standards and prepare a report on the same 5. Using any open source SIEM tool perform an analysis of an attack 6. Make a report on the SIEM online courses and certifications available 7. Make a report on SIEM best practices 8. Enumerate the various criteria to be used for selecting the best SIEM solution for an organization 9. Write a program which takes as input the requirements to be met by an SIEM tool and provides recommendations regarding the tools which fulfill the requirements 10. Take a report on SIEM use cases	
Recommended Learning Resources		
Print Resources	1. DAVID R. MILLER,SHON HARRIS,ALLEN A. HARPER,STEPHEN VANDYKE and CHRIS BLASK, "Security Information and Event Management (SIEM) Implementation", by The McGraw-Hill Companies, 2011. 2. Mark Talabis , Robert McPherson, Inez Miyamoto and Jason Martin , “Information Security Analytics: Finding Security Insights, Patterns, and Anomalies in Big Data”, Syngress, 2014.	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

<table>
<tr><td>Year</td><td>IV</td><td colspan="2" rowspan="2">Course Code : CSCY406

Course Title : Machine Learning for Cybersecurity</td><td>Credits</td><td>4</td></tr>
<tr><td rowspan="2">Sem.</td><td rowspan="2">VII</td><td>Hours</td><td>75</td></tr>
<tr><td>Category</td><td>C</td></tr>
<tr><td>Course Prerequisites if any</td><td colspan="5">● Basic knowledge of Cybersecurity</td></tr>
<tr><td>Internal Assessment Marks: 25</td><td colspan="2">End Semester Marks: 75</td><td colspan="3">Duration of ESA (Theory) : 03 hrs.
Duration of ESA (Practical) : 03 hrs.</td></tr>
<tr><td>Course Outcomes</td><td colspan="5">● Understanding basics of how machine learning is useful for Cybersecurity
● Understanding the application of various machine learning algorithms for Cybersecurity issues
● Applying machine learning for various cybersecurity applications
● Developing machine learning based cybersecurity applications
● Identifying new applications of machine learning for cybersecurity</td></tr>
<tr><td>Unit No.</td><td colspan="3">Course Content</td><td>Hours</td></tr>
<tr><td colspan="5">Theory Component</td></tr>
<tr><td>Unit I</td><td colspan="3">Basics of Machine Learning in Cybersecurity
Machine learning in cybersecurity, Current cybersecurity solutions, Data in machine learning, Different types of machine learning algorithm, Algorithms in machine learning, The machine learning architecture - Data ingestion, Data store, The model engine, Data preparation, Feature generation, Training Testing - Hands-on machine learning, Python for machine learning.</td><td>9</td></tr>
<tr><td>Unit II</td><td colspan="3">Time Series Analysis
Time series analysis - Stationarity of a time series models ,Strictly stationary process, correlation in time series - Classes of time series models - Stochastic time series model, Artificial neural network time series model Support vector time series models, Time series components - Time series decomposition - Level, Trend, Seasonality, Noise - Use cases for time series - Signal processing, Stock market predictions, Weather forecasting, Reconnaissance detection - Time series analysis in cybersecurity.</td><td>9</td></tr>
<tr><td>Unit III</td><td colspan="3">Segregating Legitimate and Lousy URLs
Introduction to the types of abnormalities in URLs - URL blacklisting - Using heuristics to detect malicious pages - Data for the analysis, Feature extraction, Web content based features, Host based features, Site popularity features - Using machine learning to detect malicious URLs - Logistic regression to detect malicious URLs - SVM to detect malicious URLs – Multiclass classification for URL classification.</td><td>9</td></tr>
<tr><td>Unit IV</td><td colspan="3">Knocking Down CAPTCHAs
Characteristics of CAPTCHA - Using artificial intelligence to crack CAPTCHA -Types of CAPTCHA - reCAPTCHA, Breaking a CAPTCHA, Solving CAPTCHAs with a neural network, Dataset, Packages, Theory of CNN, Model - Code - Training the model, Testing the model .</td><td>9</td></tr>
</table>

Unit V	**Using Data Science to Catch Email Fraud and Spam** Email spoofing - Bogus offers, Requests for help, Spam Detection- Types of spam emails, Types of mail servers, Data collection from mail servers , Using the Naive Bayes theorem to detect spam, Laplace smoothing, Featurization techniques that convert text-based emails into numeric values - Logistic regression spam filters.	9
Practical Component		
Practical Component:	Perform the following using any **two** appropriate cybersecurity data sets. 1. Time series analysis of an attack data 2. Reconnaissance detection 3. Classification of malicious and legitimate URLs using various classification algorithms 4. Breaking / solving Captchas 5. Classifying spam Emails	
Recommended Learning Resources		
Print Resources	1. Soma Halder and Sinan Ozdemir, "Hands-On Machine Learning for Cybersecurity" , Packt Publishing, 2018. 2.Emmanuel Tsukerman, "Machine Learning for Cybersecurity Cookbook" , Packt Publishing, 2019.	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

Year	IV	Course Code: CSCY407	Credits	4
Sem.	VII		Hours	75
		Course Title: Threat Intelligence	Category	C

Course Prerequisites, if any	● Knowledge of Cybersecurity	
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory) : 03 hrs. Duration of ESA (Practical) : 03 hrs.
Course Outcomes	● Understanding the basics of threat intelligence ● Learning the how threat intelligence helps for incident response and vulnerability management ● Comprehending how threat intelligence helps for risk analysis ● Learning to use threat intelligence for fraud detection ● Applying threat detection for new cybersecurity attack detection or prevention scenarios	

Unit No.	Course Content	Hours
	Theory Component	
Unit I	**Threat Analysis and Threat Intelligence Model Formulation** Threat Modeling, Understanding the threat modeling process, Threat modeling methodologies - Good Intelligence, Bad Intelligence, Comparison of Good and Bad Intelligence, Contrasting Good from Bad intelligence, Effects of both Good and Bad intelligence.	9
Unit II	**Adversary Data Collection Sources And Adversarial Data Extraction** Adversary-based threat modeling, Adversary goals, Adversary targets, Adversary constraints, Adversary resources-Pivot Off and Extracting Adversarial Data- Adversary goals as a data source, Setting up a mitigation plan .	9
Unit III	**Security Compromise Indicators and Threat Assessments** Common indicators of compromise, Challenges of IOCs, Tactics, Techniques, and Procedures (TTP) - Data correlation, Creating system log entry files data , Creating unusual outbound traffic,Key Windows Services - Conduct Threat Assessments In Depth - Malware analysis , SQL injections analysis	9
Unit IV	**Heat Maps, Infographics & Dashboards and Threat Intelligence System** Heat map - 2D density plots , when to use, Practices for using heat maps , Common heat map options and Visualization tools - Build Reliable & Robust Threat Intelligence System - Planning and direction, collection, processing, Analysis, Dissemination.	9
Unit V	**Statistical Approaches And Analytical Skills for Threat Intelligence and Planning for Disaster** Statistical Approaches for Threat Intelligence - Data preparation , classification , validation, correlation and scoring - Develop Analytical Skills for Complex Threats - Understanding analytical	9

	skills, common threats, threat objectives, threat mitigation methods and tools, Adversary attack vectors - **P**lanning for Disaster - APTS, Zero-day vulnerabilities , zero-day threats , Planning against APT attacks	
Practical Component		
Practical Component:	1. Formulate a Full STRIDE Threat Modelling system and prepare a report on the same 2. Send Phishing Mails for Social Engineering 3. Analyzing Phishing Emails that you've received in past two years and prepare report on the same 4. Familiarize with Binalyze Tactical software for various Digital Forensics and Incident Response activities 5. Find unwanted applications / software in your Windows PC, eliminate it and prepare a report on the same 6. Perform a basic malware analysis on a suspicious file in your system and prepare a report on the same 7. Create Heat Maps using any chosen dataset on cybercrimes with the following: a. Microsoft Excel b. Maltego 8. Review the key considerations for the five phase of the Threat Intelligence Lifecycle 9. Find the vulnerabilities via Internet using Shodan And Google Hacking Techniques	30
Recommended Learning Resources		
Print Resources	1. Erdal Ozkaya, " Practical Cyber Threat Intelligence", BPB Online, 2022. 2. Zane Pokorny and Christopher Ahlberg " The Threat Intelligence Handbook: Moving Toward a Security Intelligence Program",CyberEdge Press, 2019. 3. Chris Pace and Christopher Ahlberg, "The Threat Intelligence Handbook: A Practical Guide for Security Teams to Unlocking the Power of Intelligence",CyberEdge Press , 2018.	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

SEMESTER VIII

Year	IV	Course Code: CSCY408	Credits	4
Sem.	VIII	Course Title : Blockchain Technologies	Hours	75
			Category	C
Course Prerequisites, if any	● Knowledge of programming, cybersecurity and cryptography			
Internal Assessment Marks: 25	End Semester Marks: 75		Duration of ESA (Theory) : 03 hrs. Duration of ESA (Practical) : 03 hrs.	
Course Outcomes	● Understanding the fundamentals and importance of blockchain technology ● Evaluating and selecting the appropriate blockchain platform ● Deploying blockchain tools and getting started with Chain on Azure ● Exploring the role of blockchain in smart city development ● Understanding the use of Blockchain in Fintech			

Unit No.	Course Content	Hours
	Theory Component	
Unit I	**Introducing Blockchain** Structure of Blockchain-Blockchain Applications-Blockchain Life Cycle-Driving Force of Blockchains-Blockchains in Use-Picking a Blockchain-Adding Substance-Determining Needs-Defining Goals-Choosing a Solution-Getting Hands-on Blockchain - Diving into Blockchain Technology - Securing and Exchanging Your Cryptocurrency	9
Unit II	**Beholding the Bitcoin Blockchain** Bitcoin: The New Wild West- Encountering the Ethereum Blockchain- Hacking a Blockchain - Hacking a Blockchain- Creating Your Own ERC20 Tokens	9
Unit III	**Getting your Hands on Hyperledger** Working with Hyperledger Besu - Applying Microsoft Azure - Building in the Azure Ecosystem- Deploying Blockchain Tools on Azure- Getting Started with Chain on Azure	9
Unit IV	**Financial Technology** Future Banking Trends-Global Financial Products-Squeezing Out Fraud-Real Estate Innovations-Eliminating Title Insurance-Mortgages in the Blockchain World-Forecasting Regional Trends	9
Unit V	**Tailoring Coverage** Internet of Things in Insurance-Removing Third Parties-Global Regulatory Landscape-Smart Cities in Asia-Financial Capital Competition-Border Security	9
	Practical Component	
Practical Component:	1. Implement Blockchain with Geth 2. Simulating Blockchain Life Cycle with Ganache 3. Using any cryptocurrency exchange like blockchain.com, study the top 5 cryptocurrency prices for a week's period and plot their price variations in a graph 4. Create a wallet using Open Source tools 5. Analyzing transactions, blocks, and network activity on the Bitcoin blockchain and understanding the volatility, market trends, and trading patterns of Bitcoin 6. Implementing Hyperledger Besu on Azure Using Open Source Software	30

	7. Setting up a Hyperledger Fabric network 8. Create a simple block chain application 9. Develop a simple smart contract 10. Create a simple Defi application	
Recommended Learning Resources		
Print Resources	1. Tiana Laurence, “Blockchain for dummies” , John Wiley & Sons, 2023. 2. Lorne Lantz, Daniel Cawrey, “Mastering Blockchain”, O'Reilly Media, 2020.	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

<table>
<tr><td>Year</td><td>IV</td><td colspan="2" rowspan="2">Course Code: CSCY409

Course Title: Cyber Law</td><td>Credits</td><td>4</td></tr>
<tr><td rowspan="2">Sem.</td><td rowspan="2">VIII</td><td>Hours</td><td>75</td></tr>
<tr><td>Category</td><td>A</td></tr>
<tr><td>Course Prerequisites, if any</td><td colspan="5">● Knowledge of cybersecurity</td></tr>
<tr><td>Internal Assessment Marks: 25</td><td colspan="2">End Semester Marks: 75</td><td colspan="3">Duration of ESA (Theory): 03 hrs.</td></tr>
<tr><td>Course Outcomes</td><td colspan="5">● To learn about the cyber law and protection law of India
● Understanding cybercrimes
● Learning data protection & privacy laws
● Understanding ethical considerations in cyber laws
● To study and compare the cyber data protection laws of various countries</td></tr>
<tr><td>Unit No.</td><td colspan="3">Course Content</td><td colspan="2">Hours</td></tr>
<tr><td colspan="6">Theory Component</td></tr>
<tr><td>Unit I</td><td colspan="3">Introduction to Cyber Law
Evolution of Cyber Law-Importance and scope of Cyber Law-Objectives and purpose of Cyber Law - Legal Framework - IT Act, 2000 (India) and equivalent laws - Cybercrime laws and offenses - Data protection and privacy laws-Jurisdictional issues in cyberspace</td><td colspan="2">9</td></tr>
<tr><td>Unit II</td><td colspan="3">Cybercrimes
Types of cybercrimes (hacking, phishing, identity theft, etc)-Legal provisions related to cyber crimes - Investigation and prosecution of cybercrimes - International cooperation in combating cybercrimes</td><td colspan="2">9</td></tr>
<tr><td>Unit III</td><td colspan="3">Data Protection and Privacy
Principles of data protection - Personal data protection laws - GDPR (General Data Protection Regulation) or equivalent regulations - Data breaches and incident response</td><td colspan="2">9</td></tr>
<tr><td>Unit IV</td><td colspan="3">E-Commerce and Digital Signatures
Legal aspects of e-commerce - Electronic contracts and their validity - Digital signatures and their legal recognition - Intellectual Property in Cyberspace - Copyright issues in the digital era - Patent issues related to software and business methods</td><td colspan="2">9</td></tr>
<tr><td>Unit V</td><td colspan="3">Cyber Ethics
Ethical considerations in cyberspace - Cyberbullying and online harassment - Netiquette and responsible online behavior - Emerging Issues - Artificial Intelligence and legal implications - Blockchain and smart contracts - Internet of Things (IoT) and legal challenges</td><td colspan="2">9</td></tr>
<tr><td colspan="6">Practical Components</td></tr>
</table>

Practical Component	1. Research and present a case study showing how Cyber Law protects individuals online 2. Create a short quiz highlighting key points of the IT Act, 2000 in India 3. Identify common cyber crimes from news articles and discuss preventive measures 4. Role-play reporting a cybercrime to law enforcement, highlighting the steps involved 5. Conduct a survey on data privacy concerns among peers and present findings 6. Create a poster outlining tips for protecting personal data online 7. Design a simple online store and outline legal requirements for selling products online 8. Practice creating a digital signature using online tools and share experiences 9. Discuss online etiquette and responsibilities in a group setting, sharing personal experiences 10. Brainstorm ways to promote online safety and respect in a school or community setting
Recommended Learning Resources	
Print Resources	1. Dr. Pavan Duggal, "Cyber Law", 3rd Edition, Universal LexisNexis. 2. Brian Craig,"Cyberlaw" , Pearson Education (US), 2012.
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***	

Year	IV	Course Code: CSCY410	Credits	4
Sem.	VIII		Hours	75
		Course Title : Database and Application Security	Category	C

Course Prerequisites, if any	● Knowledge of Database Management Systems, Database Administration and Cybersecurity	
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory) : 03 hrs. Duration of ESA (Practical) : 03 hrs.
Course Outcomes	● Understand the basics of database and application security ● Learn the various configurations and settings for achieving database security ● Comprehend the various application security attacks ● Understand the countermeasures to handle application security attacks ● Able to manage the database and application security on database and application servers	

Unit No.	Course Content	Hours
	Theory Component	
Unit I	**Database Security** Introduction to database Security – Security in Information Technology – importance of data – data review – identity theft – levels of security – Human level: Corrupt/careless user, Network/User Interface, Database application program, Database system, Operating System, Physical level	9
Unit II	**Authentication and Authorization** Passwords, Profiles, Privileges and Roles - Authentication – operating system authentication, database authentication, Network or third-party authentication, Database vector password policies -Authorization – User Account authorization - Database/Application Security - Limitations of SQL Authorization – Access Control in Application Layer - Oracle Virtual Private Database – Privacy.	9
Unit III	**Securing Database to Database Communications** Monitor and limit outbound communications – secure database links – protect link usernames and passwords – monitor usage of database links – secure replication mechanisms - map and secure all data sources and sinks. Trojans – four types of database Trojans.	9
Unit IV	**Encrypting and Auditing the Data** Encrypting data in transit – encrypting data at rest – auditing architectures – audit trail – architectures of external audit systems - archive auditing information – secure auditing information – audit the audit system.	9
Unit V	**Application Security & Vulnerabilities** Application Security – Application Vulnerabilities - OWASP Top 10 Web Security Vulnerabilities - Unvalidated input, Broken access control, Broken account/session management, Cross-site scripting (XSS) flaws, Buffer overflows - SQL Injection flaws, Improper error handling, Insecure storage, Denial-of service, Insecure configuration management – Insecure File Handling.	9

Practical Component		
Practical Component:	1. Study various potential security threats to a database and prepare a report on the same 2. Create user accounts with different privileges and test their access 3. Set up and test row-level security using Oracle Virtual Private Database (VPD) 4. Establish a secure connection between two databases using database links 5. Encrypt a column of sensitive data in a database table 6. Enable auditing on a database and review the audit logs 7. Test a web application for SQL Injection and fix the vulnerability 8. Check and adjust database security settings to recommended configurations 9. Identify a potential Trojan in a database and describe steps to remove it. 10. Set up secure file storage for a database and test access control	30
Recommended Learning Resources		
Print Resources	1. Ron Ben-Natan, "Implementing Database Security and Auditing: A Guide for DBAs, Information Security Administrators and Auditors", Published by Elsevier, 2014. 2. Silvana Castano, "Database Security", Published by Addison-Wesley, 1994.	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

Year	IV	Course Code: CSCY411	Credits	4
Sem.	VIII		Hours	75
		Course Title : Data Privacy	Category	A
Course Prerequisites, if any	● Knowledge of cybersecurity, cyber laws			
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory) : 03 hrs.		
Course Outcomes	● Understanding of Data Privacy Laws and Regulation ● Learning Ethical Considerations in Data Handling ● Understanding implementing Privacy by Design Principles ● Performing Privacy Impact Assessments (PIAs) ● Familiarising Legal and Ethical Implications of Data Sharing			

Unit No.	Course Content	Hours
	Theory Component	
Unit I	**Data Governance and Simple Privacy Approaches** Data Governance, Identifying Sensitive Data, Identifying PII- Documenting Data for Use- Basic Data Documentation, Finding and Documenting Unknown Data, Tracking Data Lineage, Data Version Control, Basic Privacy: Pseudonymization for Privacy by Design.	9
Unit II	**Anonymization** Introduction to anonymization, Defining Differential Privacy - Understanding Epsilon, Differential Privacy Guarantee- Understanding Differential Privacy, Differential Privacy in Practice, Differential Privacy with the Laplace Mechanism- Differential Privacy with Laplace: A Naive Attempt, Sensitivity and Error, Privacy Budgets and Composition, Gaussian Noise for Differential Privacy- Comparing Laplace and Gaussian Noise, Real-World Differential Privacy, Sensitivity and Privacy Units, k-Anonymity.	9
Unit III	**Building Privacy into Data Pipelines** How to Build Privacy into Data Pipelines – Design Appropriate Privacy Measures, Meet Users Where They Are, Engineer Privacy In, Test and Verify- Engineering Privacy and Data Governance into Pipelines- Data Sharing Workflow, Adding Provenance and Consent Information to Collection,- Using Differential Privacy Libraries in Pipelines- Collecting Data Anonymously	9
Unit IV	**Privacy Attacks** Privacy Attacks: Analysing Common Attack Vectors , Netflix Prize Attack, Linkage Attacks, Singling Out Attacks, Strava Heat Map Attack, Membership Inference Attack, Inferring Sensitive Attributes, Other Model Leakage Attacks, Model-Stealing Attacks, Attacks Against Privacy Protocols, Data Security - Access Control, Data Loss Prevention, Extra Security Controls.	9

Unit V	**Navigating the Legal Side of Privacy** GDPR – Fundamental Data Rights Under GDPR - Data Controller Versus Data Processor, Applying Privacy-Enhancing Technologies for GDPR, Applying Privacy-Enhancing Technologies for GDPR, GDPR's Data Protection - Working with Legal Professionals, Adhering to Contractual Agreements and Contract Law, Interpreting Data Protection Regulations- Data Governance 2.0.	9
Practical Component		
Practical Component:	1. Identify and document sensitive data and Personally Identifiable Information (PII) in a given dataset 2. Study about the data privacy laws of any 5 countries and prepare a report on the same 3. Study about the data anonymization tools and prepare a report on the same 4. Apply Data Anonymization on a dataset using the above tools and prepare a report on the same 5. Apply differential privacy to a dataset and explain what epsilon is 6. Study about various data privacy attacks that happened across the globe in the past 5 years and prepare a report on the same 7. Take a dataset and identify the data privacy attacks that are applicable to it 8. Use k-anonymity to anonymize a small dataset 9. List the fundamental data rights under GDPR and apply them to a sample dataset 10. Study about Data Governance 2.0 and prepare a report on the same	30
Recommended Learning Resources		
Print Resources	1. Jarmul, K. (n.d.). Practical data privacy : enhancing privacy and security in data, 2023. 2. "Data Privacy. Foundations, New Developments and the Big Data Challenge" by Vicen Torra, Springer 2017	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

Year	IV	Course Code : CSCY412	Credits	4
Sem.	VIII	Course Title : Cybersecurity Risk Management	Hours	75
			Category	A
Course Prerequisites, if any	● Knowledge of computer networks and cybersecurity and cybersecurity management			
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory): 03 hrs.		
Course Outcomes	● Understand the IT components ● Apply Asset evaluation methods ● Apply threat modeling methods ● Apply the elements of Risk Assessment techniques ● Apply business continuity components			

Unit No.	Course Content	Hours
	Theory Component	
Unit I	**IT Systems** Information Systems - System components - network components - Risk management - What is Risk - profile - identification -assessment -Analysis -Response - Tolerance - Risk types - inherent risk - control risk - audit risk. -Security risk analysis - Advantages	9
Unit II	**IT Assets** Assets management - Identify Assets - Asset classification - Asset valuation - Binary Asset Valuation - Rank-Based Asset Valuation - Consensus Asset Valuation - Classification-Based Asset Valuation	9
Unit III	**Cyber Threat** Threat management - Identifying Threats -Threat model - Threat attributes - Attack tree - STRIDE - DREAD - OCTAVE - CAPEC- Threat Statements- Technical Threats and Safeguards - Physical Threats and Safeguard - Human Threats to Physical Security - The RIIOT Method: Physical Data Gathering - Test Physical Security Safeguard.	9
Unit IV	**Risk Assessment** Security Risk Assessment - Quantitative vs. Qualitative Analysis - Determining Risk - Creating Risk Statement - Security Risk Mitigation - Selecting Safeguard - Security Risk Assessment Reports - Report Structure.	9
Unit V	**Business Continuity** Principles of Business continuity - Business Interruption Events – Business impact assessment – fire exposure analysis – functional analysis – compliance issues – Pre-Planning - Initial Response - Recovery - Identification of Recovery environment - Identification of Recovery Point - Equipment and technology – process equipment - Business continuity	9

	plans – crisis management plans – function restoration plans – disaster recovery plans	
Practical Component		
Exercises	1. Study the IT Assets of a banking system and identify the risk type faced by each of it and prepare a report on the same 2. Perform Asset Valuation using Binary, Rank-Based , Consensus and Classification based Valuation methods on the above assets 3. Create a threat Model for the above using a. STRIDE b. DREAD c. OCTAVE 4. Perform a Security Risk Assessment on the above identified assets and prepare a report on the same 5. Suggest suitable risk mitigation methods for the identified assets 6. Identify the various Business Interruption events and perform a Business Impact Assessment for the online banking business 7. Formulate a Disaster recovery plan for Online Banking Business	30
Recommended Learning Resources		
Print Resources	1. Thomas L Norman., Risk analysis and Security countermeasure selection , CRC press, 2015. 2. Ariel Evans, Managing Cyber Risk, Routledge, 2019. 3. Lee T Ostrom, Risk Assessment: Tools, Techniques, and Their Applications, Wiley, 2019.	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

Year	IV	Course Code: CSCY413	Credits	4
Sem.	VIII	Course Title: Information Systems Audit	Hours	75
			Category	A
Course Prerequisites, if any	● Knowledge of networks, information systems, cybersecurity and cybersecurity standards			
Internal Assessment Marks: 25	End Semester Marks: 75	Duration of ESA (Theory): 03 hrs.		
Course Outcomes	● Understand the basics of Information Systems audit ● Learn the various aspects of informations Systems audit ● Learn the various aspects of an information system to be audited ● Familiarize the standards available for Information Systems audit ● Able to perform Information Systems audit as per required standards			

Unit No.	Course Content	Hours
	Theory Component	
Unit I	**Information Systems Audit Standards** Practices and Information System Security and Control Practices: Standards and Guidelines for IS Auditing -The Control Objectives - Other Laws and Regulations	9
Unit II	**Auditing Information Systems Organization and Management** Information Systems Strategies to achieve business management objectives - Policies and Procedures - Information Systems Management Practices - Organizational Structure - Audit and Evaluation Techniques	9
Unit III	**Auditing the Information Systems Process** Information Systems Hardware Platform - Information Systems Software Platform - Information Systems Network and Telecommunication Infrastructure - Information System Operational Practices	9
Unit IV	**Information Systems Integrity, Confidentiality & Availability** Logical Access Controls - Physical Access Controls - Environmental Controls - Data validation, processing and balancing controls - Business Continuity Planning and testing	9
Unit V	**Auditing Information Systems Software Development** Acquisition and Maintenance- System Integration Concepts - SDAM Methodologies - SDAM Practices - Information Systems Maintenance Practices	9
	Practical Component	
Exercises	1. Perform a study of the various open source information systems or information security auditing tools 2. Choose any 3 tools and perform the audit of the following with varying system and browser configuration settings	30

	i) A Windows Desktop / Laptop system ii) A Unix / Linux Desktop / Laptop system iii) A Linux / Windows server system 3. Prepare a checklist for the compliance of an organization's Information system corresponding to ISO 27001 standard which will help an Information System Auditor to perform the audit	
Recommended Learning Resources		
Print Resources	1. Principles of Information Security, by Michael E. Whitman and Herbert J. Mattord, Thomson Course Technology, 2022, ISBN: 0619063181 2. Information Security Management Handbook, by Richard and James Tiller , Auerbach Publication, 2013. *3.* Handbook of IT Auditing, D.Warren, L.Edelson, X.Parker, Coopers & Lybrand LLP, Warren, Gorham & Lamont. Boston, 1995 with 1999 supplement.	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

<table>
<tr><td>Year</td><td>IV</td><td colspan="2" rowspan="2">Course Code: CSCY414

Course Title: Security Operations Center</td><td>Credits</td><td>4</td></tr>
<tr><td rowspan="2">Sem.</td><td rowspan="2">VIII</td><td>Hours</td><td>75</td></tr>
<tr><td>Category</td><td>A</td></tr>
<tr><td>Course Prerequisites, if any</td><td colspan="5">● Knowledge of Networks and Cybersecurity</td></tr>
<tr><td>Internal Assessment Marks: 25</td><td colspan="2">End Semester Marks: 75</td><td colspan="3">Duration of ESA (Theory): 03 hrs.</td></tr>
<tr><td>Course Outcomes</td><td colspan="5">● Learn about Security Operations Centre (SOC)
● Understand the procedures involved in setting up an SOC
● Comprehend the various services provided by the SOC
● Familiarize the various job roles involved in an SOC
● Acquire knowledge to work in an SOC</td></tr>
<tr><td>Unit No.</td><td colspan="3">Course Content</td><td colspan="2">Hours</td></tr>
<tr><td colspan="6">Theory Component</td></tr>
<tr><td>Unit I</td><td colspan="3">Introducing Security Operations and the SOC
Factors Leading to a Dysfunctional SOC, Cyberthreats, Fundamental Security Capabilities, Standards, Guidelines and Frameworks, Industry Threat Models, Vulnerabilities and Risk, Business Challenges, In-House vs. Outsourcing, SOC Services, SOC Maturity Models, SOC Goals Assessment, SOC Capabilities Assessment, SOC Development Milestones.</td><td colspan="2">9</td></tr>
<tr><td>Unit II</td><td colspan="3">Developing a Security Operations Center
SOC Procedures, Security Tools, Planning a SOC, Designing a SOC Facility, Network Considerations, Disaster Recovery, Security Considerations, Internal Security Tools, Guidelines and Recommendations for Securing SOC Network, SOC Tools.</td><td colspan="2">9</td></tr>
<tr><td>Unit III</td><td colspan="3">SOC Services
Fundamental SOC Services, The Three Pillars of Foundational SOC Support Services, SOC Service Areas, SOC Service Job Goals, Service Maturity, SOC Service 1, SOC Service 2, SOC Service 3, SOC Service 4, SOC Service 5, SOC Service 6, SOC Service 7, SOC Service 8.</td><td colspan="2">9</td></tr>
<tr><td>Unit IV</td><td colspan="3">People and Process
Career vs. Job, Developing Job Roles, SOC Job Roles, NICE Cybersecurity Workforce Framework, Role Tiers, SOC Services and Associated Job Roles, Soft Skills, Security Clearance Requirements, Pre-Interviewing, Interviewing, Onboarding Employees, Managing People, Job Retention, Training, Certifications, Company Culture.</td><td colspan="2">9</td></tr>
<tr><td>Unit V</td><td colspan="3">Centralizing Data
Data in the SOC, Data-Focused Assessment, Logs, Security Information and Event Management, Troubleshooting SIEM Logging, APIs, Big Data, Machine Learning.</td><td colspan="2">9</td></tr>
<tr><td colspan="6">Practical Component</td></tr>
<tr><td>Exercises</td><td colspan="3">1. Conduct a tabletop exercise simulating a cyberattack and discuss SOC response</td><td colspan="2">30</td></tr>
</table>

	2. Explore a basic security monitoring tool (like Security Onion or Wireshark) to understand its functions 3. Draft incident response procedures for common cybersecurity incidents 4. Design a simple layout for a SOC room, considering space and equipment 5. Implement basic services like incident monitoring using open-source tools like OSSEC or Suricata. and evaluate their effectiveness 6. Assess current SOC services and propose improvements 7. Assign roles (e.g., incident responder, analyst) for a simulated incident response 8. Develop a training plan covering essential skills for SOC roles 9. Collect and analyze logs from sample systems using ELK stack (Elasticsearch, Logstash, Kibana) for log management 10. Explore a SIEM tool's interface and functions through guided exercises using tools like Splunk or Elastic SIEM	
Recommended Learning Resources		
Print Resources	1. Joseph Muniz - The Modern Security Operations Center_ The People, Process, and Technology for Operating SOC Services-Addison-Wesley, 2021. 2. Joseph Muniz, Gary McIntyre, Nadhem AlFardan,"Security Operations Center: Building, Operating, and Maintaining your SOC", Cisco Press, 2015	
Syllabus Design: Dr. T. Chithralekha, Professor, PUDoCS ***Dr. G. Krishnapriya, Assistant Professor, PUDoCS***		

MLD COURSES

<table>
<tr><td>Year</td><td>I / II</td><td colspan="2" rowspan="2">Course Code: COMS101</td><td>Credits</td><td>3</td></tr>
<tr><td>Sem.</td><td>I / III</td><td>Hours</td><td>60</td></tr>
<tr><td colspan="3">Course Title: Introduction to Python Programming</td><td>Category</td><td>A</td></tr>
<tr><td>Course Prerequisites, if any</td><td colspan="5">Problem-solving skills</td></tr>
<tr><td>Internal Assessment Marks: 25</td><td colspan="2">End Semester Marks: 75</td><td colspan="3">Duration of ESA (Theory): 03 hrs.</td></tr>
<tr><td>Course Outcomes</td><td colspan="5">• Understand Python programming constructs
• Learn about different data structures in Python
• Write programs using functions
• Explore the use of Python modules and packages
• Perform Visualization using Python package</td></tr>
<tr><td>Unit No.</td><td colspan="3">Course Content</td><td colspan="2">Hours</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td>Unit I</td><td colspan="3">Introduction
Python Basics: Working – Identifiers – Comments – Types – Operations – Buit-in, library functions - Strings: Accessing – Properties – Operations - Control-flow Instructions: Decision Control – logical operators – conditional expressions Repetition control instruction – break and continue – pass Statement</td><td colspan="2">12</td></tr>
<tr><td>Unit II</td><td colspan="3">Console Input/Output
Console Input – Console Output – Formatted printing – Lists - Definition – Accessing – Operations – Methods – Varieties – Comprehension – Tuples - Definition – Accessing – Operations – Varieties – Comprehension – Conversion – Iterators and Iterables - zip()</td><td colspan="2">12</td></tr>
<tr><td>Unit III</td><td colspan="3">Sets
Definition – Accessing – Operations – Functions – Mathematical set operations – Updating set operations Dictionaries - Definition – Accessing – Operations – Functions – Nested Dictionary</td><td colspan="2">12</td></tr>
<tr><td>Unit IV</td><td colspan="3">Functions
Definition – Communication – Types – Unpacking – Lambda, Recursive functions - Modules and Packages - Creation and importing</td><td colspan="2">12</td></tr>
<tr><td>Unit V</td><td colspan="3">Exception handling
Syntax errors – handling exceptions – try-except – user-defined exceptions – else, finally blocks – Tips - Visualization - Matplotlib package – Plotting Graphs</td><td colspan="2">12</td></tr>
<tr><td colspan="6">Recommended Learning Resources</td></tr>
<tr><td>Print Resources</td><td colspan="5">1. Aditya Kanetkar, Yashavant Kanetkar, Let us Python, BPB Publisher, 6th Edition, 2023</td></tr>
<tr><td colspan="6">Syllabus Design: Dr. R.Sunitha, Associate Professor, PUDoCS</td></tr>
</table>

<table>
<tr><td rowspan="2">Year</td><td rowspan="2"></td><td rowspan="2">Course Code: COMS102</td><td>Credits</td><td>3</td></tr>
<tr><td>Hours</td><td>75</td></tr>
<tr><td>Sem.</td><td></td><td>Course Title: Foundations of Information Technology</td><td>Category</td><td>A</td></tr>
<tr><td>Course Prerequisites, if any</td><td colspan="4">Basic knowledge of Computers</td></tr>
<tr><td>Internal Assessment Marks: 25</td><td colspan="2">End Semester Marks: 75</td><td colspan="2">Duration of ESA (Theory): 03 hrs.</td></tr>
<tr><td>Course Outcomes</td><td colspan="4">• Familiarize the fundamentals of Information Technology.
• Understand the management of hardware and software
• Describe the basics of networking
• Discuss about data management and security aspects of data
• Ability to troubleshoot computer systems</td></tr>
<tr><td>Unit No.</td><td colspan="3">Course Content</td><td>Hours</td></tr>
<tr><td colspan="5"></td></tr>
<tr><td>Unit I</td><td colspan="3">Introduction
Overview of IT – Computer Basics – Software fundamentals – Networks & Internet – IT ethics and policies</td><td>15</td></tr>
<tr><td>Unit II</td><td colspan="3">Hardware and Software Management
Computer Assembly and maintenance - Operating Systems – Software installation and maintenance – Virtualization, Cloud Computing</td><td>15</td></tr>
<tr><td>Unit III</td><td colspan="3">Networking Essentials
Network Fundamentals - Hardware – Protocols and services – Wireless Networking – Security</td><td>15</td></tr>
<tr><td>Unit IV</td><td colspan="3">Data Management and Security
Data and fundamentals of Database – Data Backup and recovery – Cyber Security – Encryption and Cryptography</td><td>15</td></tr>
<tr><td>Unit V</td><td colspan="3">IT Support and Troubleshooting
Help desk and IT support – Troubleshooting methodologies – Diagnostic tools and utilities – Future trends in IT</td><td>15</td></tr>
<tr><td colspan="5">Recommended Learning Resources</td></tr>
<tr><td>Print Resources</td><td colspan="4">1. Floyd Fuller, Brian Larson, Computers: Understanding Technology, EMC Paradigm, 4th Edition, 2011.
2. Mike Meyers , CompTIA A+ Certification All-in-One Exam Guide, McGraw-Hill Education, 11th Edition, 2023.
3. Jeffrey S. Beasley, Piyasat Nilkaew, Networking Essentials, Prentice Hall Certification, 3rd Edition, 2012.
4. Charles J. Brooks, Christopher Grow, Philip Craig, and Donald Short , Cybersecurity Essentials, Sybex Publisher, 1st Edition, 2018.</td></tr>
<tr><td colspan="5">Syllabus Design: Dr. R.Sunitha, Associate Professor, PUDoCS</td></tr>
</table>