KANNUR UNIVERSITY

(Abstract)

Post Graduate Diploma in Cyber Security Programme at Dept. of Information Technology, Mangattuparamba Campus - Regulation, Scheme & Syllabus -Approved & Implemented w.e.f 2023 admission - Orders issued

---

ACADEMIC C SECTION

ACAD/ACAD C3/447/2023 Dated: 12.10.2023

Read:-1. GO (Ms) No 528/2022/HEDN dated 22/10/2022

2. Letter No Acad C3/20143/2022 dated 26/11/2022

3. Email dated 09/01/2023 from the Head, Dept of Information Technology, Mangattuparamba Campus.

4. UO of even number dated 30/01/2023

5. Email dated 16/09/2023 from the Head, Dept of Infotmation Technology, Mangattuparamba Campus

6. Minutes of the meeting of the Department Council dated 07/09/2023

ORDER

1. As per paper read (1) above, Govt. of Kerala granted Administrative Sanction for starting Project Mode Programme Post Graduate Diploma in Cyber Security in the Dept.of Information Technology, Mangattuparamba campus, Kannur University during the Academic Year 2022-'23.

2. As per paper read (2) above, HoD, Dept of Information Technology was requested to prepare and submit the draft Regulation & Syllabus for the aforementioned Programme along with a panel of five-member Experts to constitute a committee to scrutinize the syllabus.

3. As per paper read (3) above, HoD, Dept of Information Technology submitted the Regulation, Scheme and Syllabus for the Programme Post Graduate Diploma in Cyber Security along with a panel of five experts to scrutinize the syllabus.

4. As per paper read (4) above, a five member Expert Committee was constituted, with the Head , Dept of Information Technology as the Coordinator, to scrutinize the Regulation, Scheme & Syllabus of the programme. Head , Dept of Information Technology, was authorised to submit the final Regulation, Scheme & Syllabus of the Programme after incorporating the corrections/modifications , if any, suggested by the Expert Committee.

5 . As per paper read (5) above, Head , Dept. of Information Technology submitted the final draft Regulation, Scheme & Syllabus of Post Graduate Diploma in Cyber Security Programme incorporating the suggestions of the Expert Committee. Department Council in its meeting held on 07/09/2023 vide paper read (6) above approved the aforesaid syllabus.

6. The Vice Chancellor, after considering the matter in detail and in exercise of the powers of the Academic Council conferred under section 11(1), Chapter III of Kannur University Act 1996,

approved the Regulation, Scheme & Syllabus of Post Graduate Diploma in Cyber Security Programme subject to report to the Academic Council and accorded sanction to implement the Programme in the Department of Information Technology, Mangattuparamba Campus w.e.f 2023 admission.

10. Regulation, Scheme & Syllabus of Post Graduate Diploma in Cyber Security Programme, implemented with effect from 2023 admission, is appended and uploaded in the University website (www.kannuruniversity.ac.in)

11. Orders are issued accordingly.

Sd/-

Narayanadas K

DEPUTY REGISTRAR (ACAD)

For REGISTRAR

To: Head, Dept of Information Technology, Mangattuparamba Campus

Copy To: 1. To Exam Branch (through PA to CE)
2. PS to VC/ PA to PVC/ PA to R
3. EP IV / EXCI/SWC
4 . DR/ AR I /AR II (Acad)
5 . To Webmanager (to publish in the website)
6 . Computer Programmer
7 . SF/DF/FC

Forwarded / By Order

SECTION OFFICER

KANNUR UNIVERSITY
CIVIL STATION P.O.
KANNUR
Pin-670 002
THAVAKKARA

KANNUR UNIVERSITY

POST GRADUATE DIPLOMA IN CYBER SECURITY

Regulations and Curriculum

1.0 Introduction

The Postgraduate Diploma in Cybersecurity offers a pivotal educational opportunity, targeting IT professionals and students seeking to enhance their practical knowledge in the digital security field. The curriculum is meticulously crafted to empower students with the essential knowledge, skills, and expertise necessary to tackle the ever-evolving challenges of cyber threats, thereby enhancing the resilience and security of digital systems within our increasingly interconnected world. This two-semester PGDCS program places a significant emphasis on practical aspects of cybersecurity, producing graduates who are well-prepared for industry roles. Collaborations with leading R&D organizations and industry partners specializing in cybersecurity are envisioned to enrich the program's offerings. Expertise will be imparted through a blend of in-house faculty and external industry/R&D professionals, covering key areas such as defensive cybersecurity, application security, malware analysis, ethical hacking, cyber forensic and more .

1.1Eligibility

MCA/M.Sc. Computer Science/M.Sc. Information Technology/M. Tech. (computer science, electrical, and electronics)/MSc. Physics/M.Sc. Electronics and B. Tech. in all branches of this university or any other university or institution recognized by this university as equivalent thereto, with a minimum aggregate of 55% marks or equivalent grade. Eligibility for admission for reserved categories shall be according to the rules framed by the University from time to time.

1.2Number of Seats:

This course has an intake of 20 seats per batch, including all reservations. The number of seats reserved for various reservation categories will be as per the reservation norms of Kannur University announced from time to time. The rotation matrix of the seats in the

course will be announced at the time of notification of the program. 20 seats include 5 reserved for departmental or industry-sponsored candidates. No reservation policies are applicable for industry or department-level sponsors. In the absence of sponsored candidates, those seats will be converted to the normal admission quota, and reservation policies will be applicable to fill those merged seats, considering the total seat (15 plus unfilled sponsored seats) as a single unit. The sponsored quota admission process will be completed prior to general admission in order to merge the unfilled seats into the normal admission quota.

1.3Selection Criteria of the candidates

The selection for the course shall be based on a common admission test conducted by Kannur University. The test will last two hours and comprise 50 multiple-choice questions. The syllabus and pattern for the entrance examination will be as follows:

Sl. No	Subjects	No. of Questions
1.	Basic Knowledge in Programing (C and Python)	10
2.	Fundamental knowledge in Computer Science	15
3.	Aptitude & Mental ability	25
	Total	**50 X 4 =200 marks**
	Each Right answer will be awarded 4 Marks **Each Wrong answer will be awarded -1 Mark**	

Sponsored Candidate

Sponsored candidates need not appear for the entrance examination. An application for such a candidate should be submitted with a recommendation from the head of the institution, department, or industry in the format prescribed by the university or department. The marks obtained in the qualifying examination will be considered for preparing the rank list for sponsored seats.

1.4Course Fee Structure

Sl. No	Fee Details	Amount in Rs
1.	Registration Fee (Application fee) For SC/ST	1000/- 500/-
2.	Admission Fee	555
3.	Tuition Fee (per semester)	15,000/-
4.	Lab Fee (Per Semester)	6,000/-
5.	Library Fee (Per Semester)	325
6.	SWF	320/-
7.	Special Fee	125/-
8.	Caution Deposit (Refundable)	1000/-
9.	Student Affiliation Fee	485/-
10.	Sports Affiliation fee	245/-
11.	University Union Fee	125/-
12.	University Development fund	70/-
13.	Department development fund	1000/-
14.	Alumni Fee	100/-

2. PGDCS -Programme Structure

Program Outcomes

SL No	Outcome
PO1	**Critical Thinking**: Take informed actions after identifying the assumptions that frame our thinking and actions, checking out the degree to which these assumptions are accurate and valid, and looking at our ideas and decisions (intellectual, organizational, and personal) from different perspectives
PO2	**Problem Solving**: Identify, formulate, conduct investigations, and find solutions to problems based on in-depth knowledge of relevant domains
PO3	**Communication**: Speak, read, write and listen clearly in person and through electronic media in English/language of the discipline, and make meaning of the world by connecting people, ideas, books, media and technology.
PO4	**Responsible Citizenship**: Demonstrate empathetic social concern, and the ability to act with an informed awareness of issues
PO5	**Ethics**: Recognize different value systems including your own, understand the moral dimensions of your decisions, and accept responsibility for them.
PO6	**Self-directed and Life-long Learning**: Acquire the ability to engage in independent and life-long learning in the broadest context socio- technological changes
PO7	**Environmental Sustainability and Global Perspective:** - Develop an understanding of global standards to foster a legal environment. Learn and practice to critically analyze the legal issues from local, national and international concerns

Program Specific Out comes (PSO)

SL No	Outcome
PSO1	Create skilled professionals in the area of cyber security.
PSO2	Ensure practical experience in the areas of network security, information security, and cyber-attack detection and prevention.
PSO3	Develop experimental skills for setting up a secured IT infrastructure for an organization.
PSO4	Understanding IT Security Auditing, Cyber Law, and the IT Act.
PSO5	Imparting Digital Infrastructure Management Skill

2.1 Duration of the Course

The duration of the Post Graduate Diploma in Cyber Security shall be one (1) year of full-time study divided into two semesters. Each semester should have 25 weeks, including examinations.

2.2 Course Structure

This course contains a total of eight modules in the first semester and two modules in the second semester, followed by 300 hours of real-time project work using any of the topics

studied to earn the diploma. All these components are mandatory for the completion of the course. The course comprises 30 hours (56 hours) per week, comprising 22 weeks of teaching and learning activities and 3 weeks for examination.

2.3Credits

One credit of the course is defined as a minimum of one hour of lecture or a minimum of two hours of lab or tutorial per week for 25 weeks in a semester. The minimum number of credits required to complete the Postgraduate Diploma in Cyber Security program is 44.

2.4 Seminar

Each student should select a relevant topic and prepare a seminar report for each theory course under the guidance of a faculty member. Students should prepare an abstract of the topic and distribute it to every faculty member at least one week ahead of the seminar. The presentation shall be of a minimum of 30 minutes duration. (Mark distribution: 50% for report and 50% for presentation and discussion.)

2.5Assignments

Each student shall be required to submit a minimum of three assignments for each course. The details, such as the number of assignments, mark distribution, and weightage for each assignment, will be announced by the faculty in charge of the course at the beginning of the semester.

2.6Tests

A minimum of two class tests will be conducted for each course. The details, such as the number of tests, mark distribution, and weightage for each test, will be announced by the faculty in charge of the course at the beginning of the semester.

2.7Case studies / Lab assignments

Each student should carry out a case study or micro project for each theory subject, and an experimental or study report should be submitted to the faculty in charge for consideration against the continuous evaluation component.

2.8Attendance

The minimum attendance required for each course shall be 60% of the total number of classes conducted for each semester. Those who secure the minimum attendance in a semester alone will be allowed to register for the end-of-semester examination. Maximum of 10 days of attendance will be condoned for the entire course period (1 year) ; subjected to the approval of the Vice Chancellor. The benefit of condonation of attendance will be granted to the students on health grounds for participating in University Union activities, meetings of the university bodies, and extracurricular activities on the production of genuine supporting documents with the recommendation of the Head of the Department concerned. A student who is not eligible for condonation shall repeat the course with the subsequent batch.

3.0Evaluation

There will be two types of evaluations: continuous evaluation (CE) and end-of-semester evaluation (ESE). Continuous evaluation (CE) will be done by the faculty members who handle the course, and ESE will be conducted by the university. The proportion of the distribution of marks, including CE (continuous evaluation) and ESE (end semester examination), shall be 40:60. Students have to secure a minimum of 50 percent or an equivalent grade point for CE and ESE together for each individual course except project. For the project module, a minimum of 50% is required for both CE and ESE components separately.

3.1Continuous Evaluation (CE): Continuous Evaluation (CE) of a course shall be based on periodic written tests, assignments, seminars, viva-voce, case studies, and project work. Considering the nature of the course, the continuous evaluation (CE) components for PGDCS theory courses and laboratory courses will be as follows:

3.1.1 Components of Continuous Evaluation (Theory)

Sl. No	Component	Marks
1.	Seminar Internal	10
2.	Case studies / Project(individual)	10
3.	Assignments	05

4.	Test	15
	Total	**40**

3.1.2 Components of Continuous Evaluation (Laboratory)

Sl. No	Component	Marks
1.	Record Work/Lab Assignments	10
2.	Implementing the experiment in the Lab	15
3.	Viva-voce	15
	Total	**40**

3.2End-Semester Evaluation (ESE).

The end-semester examinations of each semester for theory and practical's, including projects, will be conducted by the Controller of Examinations.

3.2.1 End Semester Evaluation of Theory papers (ESE)

ESE-Theory examinations will be scheduled and conducted by the Controller of Examinations in consultation with the Head of the Department. The tabulation registers for each semester shall be prepared and maintained by the Examination Branch. For the evaluation of answer scripts, there shall be a minimum of one external examiner (as chief) along with the panels of internal examiners (as additional) to ensure transparency in the conduct of examinations. The external examiners will be faculty members appointed from other colleges or departments of this university or from other universities, scientists, or engineers from recognized R&D organizations. The duration of the end-of-semester examination for theory shall be 3 hours with a maximum mark of 60. The pattern of questions

will be the same as the pattern of questions for the PG-University department. Re-valuation of the answer script follows the regulations for re-valuation of PG programs in the university department.

3.2.2 End Semester Evaluation of Practical courses (ESE)

The end-semester examination for practical courses will be conducted by the controller of examinations with a duly approved panel submitted by the Head of the Department. The panel consists of one external member and one internal faculty member. The external examiner may be a faculty member of the college of Kannur University, another university, an engineer, or a scientist from a recognized R&D organization or industry.

The components for practical's will be as follows:

Sl. No	Component	Marks
1.	Record Work/Lab Assignments report	10
2.	Implementing the experiment in the Lab	20
3.	Viva-voce	10
	Total	**60**

3.3 Evaluation of Project

A project has to be undertaken by all students enrolled in the program. A project or an industry-oriented case study in the area of cyber security is a must. The hours allotted for project work may be clustered into a single slot so that students can do their work at a center or location for a continuous period of time. The major project work should be carried out in the department or institution or in an industry or R&D organization of national repute. Project work shall be carried out under the supervision of an expert in the area. If the project is carried out in an industry or R&D organization outside the campus, then a co-guide shall be

selected from the concerned organization. If the project work is of an interdisciplinary nature, a co-guide shall be taken from the other department concerned. Every student should do the project individually, and no grouping is allowed. If two or more students are engaged in a single project, it should be ensured that they work on mutually exclusive components or modules of the single project so that the project will be reported as an individual project. The candidates are required to get the synopsis approved by the department before the commencement of the project. At the end of the semester, the candidate shall submit the project report duly approved by the guide and co-guide for end-of-semester evaluation. The project report shall be prepared according to the guidelines announced by the department from time to time.

Evaluation of Project:

1. A departmental committee duly constituted by the head of the department will review the project periodically.
2. **Continuous Assessment of Project Work:** There shall be three internal presentations before the committee (minimum two members, including the guide). The assessment is based on the presentation, interim report, and viva voce. The total mark for CE shall be divided among the three presentations in the following ratio **20%:30%:50%.** Each internal presentation shall be evaluated based on the following components:

Sl.No	**COMPONENTS**	**% OF MARKS**
I	Understanding of the problem / concepts	25%
II	Adhering to methodology	20%
III	Quality of presentation and demonstration (Demonstration is	15%

	optional	
IV	Quantum of work / effort	30%
V	Organization and content of Project report	10%

3. End Semester Assessment of Project: A board of two examiners (one external and one internal) appointed by the university shall conduct the ESE evaluation. The evaluation shall be based on the report, presentation of the work, demonstration of the work, and a detailed viva voce based on the work carried out. A candidate will not be permitted to attend the project evaluation without duly certified project reports. Also, a project will be evaluated only if the candidate attends the ESE presentation and viva voce on the scheduled date and time. The end-of-semester evaluation shall consist of the following components:

	COMPONENTS	**% OF MARKS**
I	Understanding of the problem/requirements/ concepts related to the project	15
I I	Adhering to methodology (Software engineering phases or research methodology) and the candidates understanding of the components of methodology	15
I II	Quality of Modeling of the problem	20

	and solution/ database design / form design / reports / testing (For research projects - relevance /novelty of the work(s)/ use of data/ proposal of new models /analysis of algorithms/ comparison and analysis of results/findings)	
IV	Quality of presentation / demonstration	15
V	Quantum of work / effort - assessed through the content of report, presentation and viva	25
V I	Organization and content of report	10

4. A student shall pass the project course if she or he secures a separate minimum of 50% for the CE and ESE and 50% for the ESE and CE put together.
5. If a candidate fails the project evaluation, he or she has to repeat the project course along with the next batch and undergo both CE and ESE. Unlike theory and practical courses, the CE mark will not be retained.
6. There shall be no improvement chance for the marks obtained in the project course.

4.0 <u>Grading</u>

An alphabetical grading system shall be adopted for the assessment of students performance in a course. The grade is based on a ten-point scale. The following table gives the range of marks, grade points, and the alphabetical grade.

Range of marks %	**Grade points**	**Alphabetical grade**
95-100	10	O
85-94	9	A+
75-84	8	A

65-74	7	B+
55-64	6	B
50–54	5	C
Below50	0	F

A minimum of grade point 5 (grade C) is needed for the successful completion of a course.

The performance of a student at the end of each semester is indicated by the grade point average (GPA), which is calculated by taking the weighted average of the grade points of the courses successfully completed. The following formula is used for the calculation: The average will be rounded off to two decimal places.

$$\text{GPA} = \frac{\text{Sum of (grade points in a course multiplied by its credit)}}{\text{Sum of credits of courses}}$$

The overall performance of a student is indicated by the cumulative grade point average (CGPA) and is calculated using the same formula given above.

The empirical formula for calculating the percentage of marks will be CGPAx10. Based on the CGPA, the overall letter grade of the student shall be determined in the following way:

Conversion of Grades into classification

CGPA	**Overall Letter Grade**	**Classification**
9.5andabove	O	First class with exemplary
8.5 and above but less than 9.5	A+	First class with distinction
7.5 and above but less than 8.5	A	

6.5andabovebutlessthan7.5	B+	First Class
5.5andabovebutlessthan6.5	B	
5 and above but less than 5.5	C	Second class

4.1Grade Card

The Controller of Examination, Kannur University, will issue the semester-wise grade card, consolidated grade statement based on the authenticated documents submitted by the Head of the Department after the approval of the department council at the end of each semester. The Final PG Diploma certificates will be issued by the University.

5.0 Supplementary Examinations for Failed Candidates

1. Candidates who have failed (F grade) in the semester examinations (except project work) can appear for the failed papers for the particular semester along with regular However, the Continuous Evaluation (CE) marks will remain the same. Two such supplementary chances will be given for each semester within two years.
2. In the event of failure in project work, the candidate shall re-register for project work, redo the project work, and resubmit the project report fresh for evaluation. The Continuous Evaluation marks shall be freshly allotted in this case.

Appearance for continuous evaluation and end-semester evaluation is compulsory, and no grade shall be awarded to a candidate if he or she is absent for CE, ESE, or both.

A student who fails to complete the program or semester can repeat the full program or semester once if the department council permits it.

There shall be no provision for the improvement of CE marks. The maximum period for completing the PGDCS will be 2 years.

6.0 Department Council

The department council will review the course progress periodically. Any specific amendment in the syllabus, evaluation, or any other matter that is not mentioned in these

regulations related to the PGDCS course will be discussed in the department council, and suitable action will be taken.

7.0 Industrial Collaboration

As the PGDCS program is designed to nurture industry-ready professionals in the area of cyber security, it is very important to have sessions handled by experts from R&D institutes and industry who work in the area of cyber security. It is provisioned to organize a series of lecture sessions and boot camps led by experts from industry or R&D labs. Lecture sessions with hands-on activities will be organized with experts over and above the regular lecture sessions and labs. Such sessions or boot camps can be organized even on Saturdays, Sundays, and holidays, depending on the availability of the experts. An amount of Rs. 4 lakhs will be provisioned for meeting the expenditure for providing the TA/DA and remuneration to the experts. An honorarium of Rs. 2000 per hour up to a maximum of Rs. 8,000 per day can be provided to the experts. Experts are eligible for economy-class airfare, and no separate approvals are required for this. The amount earmarked for expert lectures will be transferred to the department by the finance officer within one week of the commencement of classes in every year.

8.0 Faculty and No-Teaching staff for the programme

It is proposed to have the following faculty pattern for the PGDCS program.

Designation	Number of Posts
Asst. Professor	2
Lab instructor	1

8.1Appointment of Assistant Professor (2 Nos)

Qualifications prescribed by UGC for the appointment of assistant professor shall be applicable. However, proven teaching or research experience in the area of cyber security is a

must in addition to the minimum qualification for the appointment as Asst. Professor. The assistant professor position can be filled either by direct recruitment or deputation from an R&D institution or academia.

8.3 Appointment of Lab Instructor

As provisioned in the government approval, an amount of Rs. 5 lakh is earmarked as contingent grant (for appointing support staff for the conduct of the PGDCS program). One lab instructor can be appointed for the PGDCS program with a monthly remuneration of 35,000/- Per month. This incurs an expenditure of 4,20,000/- per year.

8.3.1 Qualification for Lab Instructor

Minimum qualifications for lab instructors will be MCA/M Sc (CS) or BE/B. Tech/M Tech (Computer Science/IT/Electronics). Minimum 1 year Experience in the area of cyber security and IT infrastructure management will be desirable.

9.0 Grievance redressal

As stated in the Regulations for Postgraduate Programs Under the Choice Based Credit Semester System (CBCSS) in the Departments and Schools Effective from 2021 Admission.

COURSE STRUCTURE

Semester	Theory	Practical
Semester I	5	2
Semester II	2 electives	1 (project)

Semester I

Subject Code	Subject	*Instructional Hrs./week*			Marks			Credit
		L	**P**	**T**	**CE**	**ESE**	**Total**	
PDCS01C01	Operating System Security	4	0	0	40	60	100	4
PDCS01C02	Application and Data Security	4	0	0	40	60	100	4
PDCS01C03	Network Security	3	0	0	40	60	100	3
PDCS01C04	Ethical Hacking	4	0	0	40	60	100	4
PDCS01C05	Information Security	3	0	0	40	60	100	3
PDCS01P01	Lab –I Application and Data Security &Operating System Security	0	6	2	40	60	100	3
PDCS01P02	Lab–II Ethical Hacking & Network Security	0	6	3	40	60	100	3
Total		**18**	**12**	**5**	**280**	**420**	**700**	**24**

Semester II

Subject Code	Subject	*Instructional Hrs./week*			Marks			Credit
		L	**P**	**T**	**CE**	**ESE**	**Total**	
PDCS02E0X	Elective – 1	4	0	0	40	60	100	4
PDCS02E0X	Elective – II	4	0	0	40	60	100	4
PDCS02P01	Project	0	24	0	40	60	100	12
Total		**8**	**24**	**0**	**120**	**180**	**300**	**20**

Electives 1 & II

PDCS02E01 Security Auditing

PDCS02E02 Cyber Law and IT Act

PDCS02E03 Blockchain and Cryptocurrency Technologies

PDCS02E04 Cyber Forensic

PDCS02E05 Biometric Image Processing

PDCS02E06 Speech, Audio and Video Forensics

PDCS02E07 Machine Learning for Cyber Security

PDCS02E08 Cloud Security

SEMESTER I
CORE COURSE
PDCS01C01 Operating System and Security
Course Description

With a focus on Windows and Linux operating systems in particular, this course covers basic operating system ideas, exploring fundamental concepts such as architecture, memory management, file system management, I/O management, network operating systems, and distributed operating systems. It delves into the installation, configuration, and security of both Windows and Linux. Additionally, the course examines cloud computing and virtualization topics including zero-trust security architecture, cloud provisioning, PaaS and SaaS models, private and public cloud environments, and cloud security. The Linux module also encompasses bash scripting. A comprehensive understanding of operating systems, virtualization, cloud computing, and their corresponding security measures is provided within the course.

Course Objectives

- Provide a foundational understanding of operating systems, their functions,

  And their importance in computer systems.

- Gain knowledge of the underlying architecture and components of the Windows and Linux operating systems.
- Learning Windows and Linux operating system features—system administration and security

- Understand the fundamentals of virtualization and cloud computing.

Credit			Teaching Hours			Assessment		
L/T	P/I	Total	L/T	P/I	Total	CE	ESE	Total
4	-	4	2	2	4	40	60	100

Lecture/Tutorials, P/I=Practical/Internship, CE =Continuous Evaluation, ESE =End Semester Evaluation

COURSE OUTCOMES

Course Learning Outcomes: At the end of theCourse,theStudentwill beableto -

C01	Understand the elementary design of an operating system.
C02	Understand how to install and update Windows 11 and Server 2019, Linux and configure GRUB boot loader.
C03	Implement network connectivity and remote access solutions in Windows.
C04	Install, configure, manage, and maintain active directory domain services.
C05	Implement networking protocols and services - DHCP, DNS etc.
C06	Use Linux commands to manage files and file systems and to create user accounts and permissions.
C07	Configure basic Linux network services.
C08	Create and execute BASH scripts.
C09	Understand Cloud Computing, Cloud Types and Cloud Service Deployment Models (PaaS, SaaS) and the concept of Cloud Security.

- Course outcomes based on revised blooms taxonomy.

COURSE CONTENTS

Module 1

Fundamental operating system concept

Basic Concepts of Operating system – Architecture – Process management- Memory management- File system management- I/O Management – Basics of Network Operating Systems – Basics of Distributed Operating system.

Module 2

Windows Operating system

Windows OS History and Fundamentals-Installation of windows operating system Windows 11 and Server 2019- Updating windows system and patch management-Windows File system and Disk Management- Active Directory and windows domain-Windows Security and OS Hardening-Virtualization using Hyper-V-Network Based installation method-Network Configuring- Implementation of infrastructure of windows networks-Active Directory Domain Services (ADDS)- DNS, DHCP and IPAM, Network Policy Server (NPS), Local Policies, Group Policies, Flexible Single Master Operation (FSMO)-File Server Resource Manager (FSRM), Windows Server Backup (WSB)-Power shell Scripting, Windows Administration using power shell, Background Jobs and Remote Administration.

Module 3

Linux Operating system

Linux Fundamentals – (Startup Files, Linux boot process), Basic Commands of Linux, Installation of Linux- Configuring the GRUB boot loader, Disk management and partition, Controlling and managing Services, -Linux Authentication method and User administration-Linux File System and permissions -Methods for installation of Packages. Apt-get and YUM/DNF Package manager. Network configurations- configuration of NFS, FTP and DHCP Servers. Linux Security and OS Hardening. Virtualization using

KVM.Bash Scripting, Introduction to BASH Command Line Interface (CLI) Error Handling Debugging & Redirection of scripts, Automate Task Using Bash Script, Security patches, Logging & Monitoring using script.

Module 4

Virtualization and cloud computing

Virtualization concepts - Cloud fundamentals – architecture -Private cloud environment-Public cloud environment -Auto-provisioning-Cloud as PaaS, SaaS-Cloud computing securitization-Ethics and standard of cloud Cloud Data Security - Cloud Application Security-Zero Trust Security Architecture.

Core Compulsory Readings (Books, Journals, E-sources Websites/ weblinks)

1. “Operating System Principles, 7TH EDBook“, by AviSilberschatz, Greg Gagne, and Peter Baer Galvin.
2. “Linux: The complete reference, sixth edition “, by Richard Peterson.
3. “Virtualization and cloud computing “, by DacNhuong L, RaghvendraKumar, John Wiley and Sons.
4. “Linux with operating system concepts “, by Richard Fox.
5. “Windows operating system fundamentals “, by Christal Panek.

Core Suggested Readings (Books, Journals, E-sources Websites/ weblinks)

1. "Windows PowerShell in Action" by Bruce Payette.
2. "Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry" by Harlan Carvey.
3. "Linux Bible" by Christopher Negus.
4. “UNIX and Linux System Administration Handbook" by Evi Nemeth, Garth Snyder, Trent R. Hein, and Ben Whaley.
5. "Group Policy: Fundamentals, Security, and the Managed Desktop" by Jeremy Moskowitz.
6. "Linux Command Line and Shell Scripting Bible" by Richard Blum and Christine Bresnahan.

TEACHING LEARNING STRATEGIES

- Hands-on-oriented teaching, collaborative learning, case studies and project presentations, peer-led discussions**.**

MODE OF TRANSACTION

- Lecture, seminar, discussion, audio and video presentation, demonstration, practical assignments, and exercises.

ASSESSMENT RUBRICS

Component	**Marks**
End Semester Evaluation	**60**
Continuous Evaluation	**40**
• Seminar Internal	10
• Case studies / Project(individual)	10
• Assignments	05
• Test	15
Total	**100**

<u>Sample Questions to test Outcomes.</u>

1. How do you configure Active Directory Domain Services (AD DS) on a Windows Server?
2. How do you implement and manage Group Policies in Windows Server 2019?
3. Discuss the significance of the STP (Spanning Tree Protocol) in preventing network loops and ensuring loop-free paths in networking.

4. Explain the concept of VLAN (Virtual Local Area Network) and its implementation.

5. Discuss the usage of the "ssh" command for remote login and file transfer in Linux.

6. What are the major cloud service providers and their offerings?

7. How do you ensure security and compliance in a cloud environment?

SEMESTER I
CORE COURSE
PDCS01C02 Application and Data Security

Course Description

This course primarily focuses on web, mobile, and data-related security. It delves into the intricacies of web and mobile application security by examining various vulnerabilities within web applications, corresponding attacks, and respective countermeasures. The course imparts fundamental knowledge about the Android system and explores potential mobile app vulnerabilities and attacks. Furthermore, it comprehensively addresses data security, privacy, the significance of secure software development, and its necessity in today's world.

Course Objectives

- Understanding the security concepts related to web applications and mobile applications.
- Learning the importance of data security, the risk of attacks, and countermeasures.
- Understanding the vulnerabilities and identifying the vulnerabilities in a system and a network.
- Fundamental knowledge about the Android system and mobile application data security.
- Implementation of security software and its necessity.

Credit	Teaching Hours	Assessment

L/T	P/I	Total	L/T	P/I	Total	CE	ESE	Total
4	-	4	2	2	4	40	60	100

Lecture/Tutorials, P/I=Practical/Internship, CE =Continuous Evaluation, ESE =End Semester Evaluation

COURSE OUTCOMES

Course Learning Outcomes: At the end of the Course, the Student will be able to -

C01	Understand basics of internet and web applications.
C02	Implement OWASP Top 10-Injection attacks.
C03	Understand and implement different types of web attacks and its counter measures.
C04	Know Android architecture, file system structure and app fundamentals.
C05	Implement Android security model, device rooting and debug bridge.
C06	Familiarize the OWASP Mobile Top 10 threats.
C07	Get exposed to Data Security Concepts, Software Security, and the importance of Secure Software Development.
C08	Design software to meet software security requirements.

*Course outcomes based on revised blooms taxonomy

COURSE CONTENTS

Module 1

Introduction to Web security

Basic of Internet and Web Applications Introduction to Client Server model- Three-Tier Architecture HTML-XML basics- HTTP Protocol, HTTPS - TLS/SSL- Cookies-Sessions-Tokens-Web Proxies-Web services- API Basics – RESTAPI and RESTfulAPI

Module 2

Web Application Security

Web Application Vulnerabilities- OWASP Top 10-Injection attacks (SQL, OS, XSS and CMD, XML Injections)-Cross Site Scripting- Cross site Request Forgery - File Path Traversal-Cookie stealing- Broken Access Control -Session Hijacking-Data tampering--API Security (Postman) -Application layer DoS/DDoS- Web Attacks counter measures- Secure web server configuration-Input Validation-Web Application Firewall (WAF).

Module 3

Mobile Application Security

Introduction to Android Architecture, Android File system Structure, Android App fundamentals, and build process, Android Security Model, Device Rooting, Android Debug bridge, Penetration Testing Tools, OWASP Top 10 Mobile App vulnerabilities, Attacks on Android Apps, Web based attacks on Android devices, Networks based attacks, Social Engineering attacks, Overview of Mobile Malware, Android App Analysis- (Tool Mob safe)

Module 4

Data security and Secure Software Development Practice

Introduction to data security- (Data at rest-transit-use) Data Classification (Public – Private-Internal- Confidential, restricted) - Data Encryption- Data loss prevention- Data Privacy-Database security- Data vault – Data Security Standards- Block chain – Software Development Practice – SDLC – Secure Soft Develop Practices –Code-review- Static Analysis Security Testing Vs Dynamic Analysis Security Testing. (Tool: Sonar cube)

Core Compulsory Readings (Books, Journals, E-sources Websites/ weblinks)

1. Web Application Security: Exploitation and Countermeasures for Modern Web Application (Greyscale Indian Edition) – Andrew Hoffman.
2. Web Security for developers: Real Threats, Practical Defense by Malcom McDonald.
3. Mobile Application Security by Dwivedi and Himanshu, McGraw Hill.
4. Application Security for the Android Platform by Jeff Six.
5. Data Security: Technical and Organizational Protection measures against data loss and computer crime by Thomas H. Lenhard.

6. Introduction to Data Security and Controls by Edward R Buck.

Core Suggested Readings (Books, Journals, E-sources Websites/ weblinks)

1. Web Application Security: A Beginner's Guide" by Bryan Sullivan and Vincent Liu.
2. "The Tangled Web: A Guide to Securing Modern Web Applications" by Michal Zalewski.
3. "OWASP Testing Guide" by The Open Web Application Security Project.
4. " The Mobile Application Hacker's Handbook" by Dominic Chell, Tyrone Erasmus, Shaun Colley, and Ollie Whitehouse.
5. "iOS Application Security: The Definitive Guide for Hackers and Developers" by David Thiel.
6. "Data Protection: Governance, Risk Management, and Compliance" by Gerardus Blokdyk.
7. "Cryptography Engineering: Design Principles and Practical Applications" by Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno.
8. "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World" by Bruce Schneier.

TEACHING LEARNING STRATEGIES

Hands-on-oriented lecturing, collaborative learning, case studies and project presentations, and peer-led discussions.

MODE OF TRANSACTION

Lecture, seminar, discussion, audio and video presentation, demonstration, practical assignments, and exercises.

ASSESSMENT RUBRICS

Component	Marks
End Semester Evaluation	**60**
Continuous Evaluation	**40**

• Seminar Internal	10
• Case studies / Project(individual)	10
• Assignments	05
• Test	15
Total	**100**

Sample Questions to test Outcomes:

1.What are the common types of web application vulnerabilities and how can they be exploited?

2. What is SQL injection and how can developers protect against it in web applications?

3.Discuss the principles and importance of data classification in a data security strategy.

4.What are the common security challenges in mobile application development and deployment?

5. How can developers ensure secure communication between a mobile application and its backend servers?

6. Discuss the importance of secure session management in web applications.

SEMESTER I
CORE COURSE
PDCS01C03 Network Security

The Network Security course encompasses the essential concepts pertaining to computer networks and security issues. This course imparts foundational knowledge of computer networks, including topologies, configurations, transmission modes, media, and network protocols. Further, it examines various network protocols, services, and devices in detail. The course also addresses wireless networks, MAC addresses, IP addresses, and subnetting. Moreover, it explores perimeter security encompassing the defense-in-depth strategy and intrusion detection systems such as firewalls, honeypots, and honeynets. Lastly, the course covers fundamental aspects of cryptography, including encryption, decryption, symmetric and asymmetric key algorithms, hashing, and digital signatures.

Course Description

Course Objectives

- Develop a solid understanding of network security concepts, principles, and best practices.
- Learn about secure network architectures, network segmentation, and defense-in-depth strategies to protect networks from unauthorized access and attacks.
- Acquire skills in network monitoring, intrusion detection, and incident response techniques to detect and respond to security incidents in a timely manner.
- Identify and analyze various types of security threats and attacks, such as malware, social engineering, phishing, and denial-of-service attacks.
- Learn about securing databases and protecting sensitive information from unauthorized access, SQL injection attacks, and other database-related vulnerabilities.

Credit			**Teaching Hours**			**Assessment**		
L/T	P/I	Total	L/T	P/I	Total	CE	ESE	Total

4	-	3	2	2	4	40	60	100

Lecture/Tutorials, P/I=Practical/Internship, CE =Continuous Evaluation, ESE =End Semester Evaluation

COURSE OUTCOMES

Course Learning Outcomes: At the end of the Course, the Student will be able to -

C01	Describe how computer networks are organized with the concept of layered approach and how signals are used to transfer data between nodes.
C02	Implement a simple LAN with hubs, bridges, and switches.
C03	Learn about DNS namespace, DNS protocol and DNS resolution process.
C04	Familiarize Email protocols - Simple Mail Transfer Protocol (SMTP), Post office Protocol (POP) Multipurpose Internet Mail Extension (MIME).
C05	Understand and analyze data encryption standard.
C06	Understand and analyze public-key cryptography, RSA, and other public-key cryptosystems.
C07	Identify core issues of network protection and perimeter defense.
C08	Explain and identify types of intrusion detection systems.
C09	Secure internal networks using router and firewall technologies.

*Course outcomes based on revised blooms taxonomy

COURSE CONTENTS

Module 1

Computer Network Fundamentals:

Introduction, Basic concepts of Computer Network - Line configuration, Topology, Transmission mode, Categories of networks, Internetworks, Transmission media - Twisted pair Cable, Coaxial Cable, Optical Fiber, Satellite Communication, Cellular Telephony, Terrestrial Microwave Basics of ISO/OSI Model- TCP IP Layer- Functions of Physical Layer, Data link layer, Network layer, Transport Layer, Session Layer, Presentation Layer and Application Layer - OSI and TCP/IP models.

Module 2

Network Hardware and Protocols:

Ethernet- Basics of wireless network - ARP,–MAC Address-IP Addressing(IPV4-IPV6)-Subnetting- LAN-WAN- Network Devices Basics: Switch- Router- Basics of Wireless Network:-802.11/a/b/g/n- SSID-BSSID Routing- Static Routing-Dynamic Routing- VLAN-Application layer Protocols : Domain Name Services (DNS) and Mail services: working of DNS, Host name Resolution Name lookup with DNS, Reverse Lookup, Domain Name Servers and Zones, DNS database: SOA, NS, MX, A and PTR records, Secondary and primary DNS, Zone change notification, root servers, internet root domains,. Simple Mail Transfer Protocol (SMTP), Post office Protocol (POP) Multipurpose Internet Mail Extension (MIME), SMTP and POP3.

Module 3

Cryptography -PKI- Digital signatures

Basics of Cryptography: Encryption- Decryption-Symmetric Key (DES, AES), Asymmetric Key- (RSA, ECC) - Hashing-Public Key Infrastructure (PKI), Digital Signature- Digital certificate-SSL-TLS.

Module 4

Perimeter security

Defense in Depth Approach-Perimeter Security- Perimeter Security devices: Firewall-Types of Firewall-Next Generation Firewall-Intrusion Detection–Intrusion-Prevention- Honeynet-Honeypot-Unified Threat Management-Denial of Service-(DoS) and Distributed Denial of Service (DDoS)-Virtual Private Network-SIEM- Zero Trust.

Core Compulsory Readings (Books, Journals, E-sources Websites/ weblinks)

1. Introduction to computer network by Sanjay sharma.
2. Fundamentals of computer networks by Chandra Mohan.
3. Cryptography and Network Security by William Stallings.
4. Cryptography and network security by Marcelo Sampaio de Alencar.
5. Securing the perimeter Deploying Identity and Access Management with Free Open-Source Software by Michael Schwartz, Maciej MAchulak.

Core Suggested Readings (Books, Journals, E-sources Websites/ weblinks)

1. "Network Security: Private Communication in a Public World" by Charlie Kaufman, Radia Perlman, and Mike Speciner.
2. "Network Security Bible" by Eric Cole.
3. "Building Internet Firewalls: Internet and Web Security" by Elizabeth D. Zwicky, Simon Cooper, and D. Brent Chapman.
4. Network Perimeter Security: Building Defense In-Depth" by Saadat Malik.
5. "Building Secure and Reliable Network Applications" by Kenneth R. van Wyk and Henk G. Sol.

TEACHING LEARNING STRATEGIES

- Hands-on-oriented lecturing, collaborative learning, case studies and project presentations, and peer-led discussions.

MODE OF TRANSACTION

- Lecture, seminar, discussion, audio and video presentation, demonstration, practical assignments, and exercises.

ASSESSMENT RUBRICS

Component	Marks
End Semester Evaluation	**60**
Continuous Evaluation	**40**
• Seminar Internal	10
• Case studies / Project(individual)	10

• Assignments	05
• Test	15
Total	**100**

Sample Questions to test Outcomes.

1. What is subnetting and why is it used in IP networking?

2. What are the common network topologies and their advantages and disadvantages?

3. How does the SSH (Secure Shell) protocol provide secure remote access to network devices?

4. What is the purpose of the ICMP (Internet Control Message Protocol) and its significance in network troubleshooting?

5. What is the concept of intrusion detection and prevention systems (IDPS) and how do they contribute to network security?

6. How can network administrators protect against distributed denial-of-service (DDoS) attacks?

SEMESTER I
CORE COURSE
PDCS01C04 Ethical hacking

Course Description

The primary concepts of ethical hacking are covered in-depth in this course, with a focus on assessing vulnerabilities. The course includes foundational knowledge of cybersecurity, malware classifications, various security breach tactics, and essential ethical hacking principles. Additionally, it delves into the different categories of hackers and offers insight into Foot-printing or Reconnaissance. The course explores vulnerability assessment through specific techniques and methodologies while examining wireless hacking, applicable security tools, and corresponding countermeasures for a more formal and precise understanding.

Course Objectives

- Understanding Ethical Hacking: Gain a comprehensive understanding of the principles, methodologies, and legal implications of ethical hacking.
- Learn how to identify and assess vulnerabilities and security weaknesses in computer systems, networks, and applications.
- Understand the techniques used by attackers to exploit vulnerabilities and learn how to analyze and mitigate these exploits.
- Explore common security issues and vulnerabilities in web applications and understand how to assess and enhance their security.

Credit			**Teaching Hours**			**Assessment**		
L/T	P/I	Total	L/T	P/I	Total	CE	ESE	Total
4	-	4	2	2	4	40	60	100

Lecture/Tutorials, P/I=Practical/Internship, CE =Continuous Evaluation, ESE =End Semester Evaluation

COURSE OUTCOMES

Course Learning Outcomes: At the end of the Course, the Student will be able to -

C01	Analyze and evaluate the cyber security needs of an organization.
C02	Know about Ethical hacking and penetration testing.
C03	Gain knowledge on Foot-printing or Reconnaissance.
C04	Examine how social engineering can be done by attacker to gain access of useful & sensitive information about the confidential data.
C05	Determine and analyze various software vulnerabilities and security solutions to reduce the risk of exploitation.
C06	Understand Wireless Protocols, revealing hidden SSIDs,wireless threats,wireless hacking methodology, method to protect a wireless network.

*Course outcomes based on revised blooms taxonomy

COURSE CONTENTS

Module 1

Introduction to Cyber Security

Introduction to Cyber security: Confidentiality – Integrity- Availability -Vulnerability -Threat – risk - Security Attacks – Malware -Virus- worm-phishing- ransomware-botnet- Steganography -Intrusion-Hacking.

Module 2

Introduction to Ethical hacking

Introduction to Ethical Hacking- Types of Hacker Classes- Cyber Killchain – Reconnaissance: Foot-printing –Google hacks - Foot printing through Web Services-Foot

printing through Social Networking Sites -Website Foot printing-Email Foot printing-Who-is Foot printing- Open source Intelligence (OSNIT Frame work) .

Module 3

Vulnerability assessment

Scanning: Different scan techniques-Port scan, Host Discovery - OS Discovery (Banner Grabbing/OS Fingerprinting) - Network scan -Vulnerability Scan- Vulnerability Analysis-Common vulnerability exposures (CVE)-Buffer Overflow-Packet Sniffers- Man In The Middle attack techniques(MITM)-ARP Spoofing-DNS Spoofing-Password Cracking and counter measures- Email Hacking and counter measures- Command and Control-Privilege Escalation-Post Exploitation.

Module 4

Wireless Hacking

Wireless Concepts -Wireless Hacking - Wireless Encryption -Wireless Threats-Wireless Hacking Methodology-Wireless Hacking Tools-Bluetooth Hacking-Wireless Security Tools-- counter measures-Device Hacking and counter measures-DoS/DdoS Methods and tools.

Core Compulsory Readings (Books, Journals, E-sources Websites/ weblinks)

1. Introduction to Cyber Security concepts principles technologies and practices by Ajay Singh.
2. Cyber Security Fundamentals by Rajesh Kumar Goutam.
3. Introduction to Ethical Hacking for beginners by Subash Bahadur Thapa.
4. Ethical Hacking by Daniel G. Graham.
5. Vulnerability Analysis and Defense for the Internet by Singh A.
6. Guide to vulnerability Analysis for Computer Network and Systems by Simon Parkinson, Andrew Crampton, Richard Hill.

7. Wireless Hacking: Introduction to wireless hacking with kali Linux by Giulio D'Agostino.

Core Suggested Readings (Books, Journals, E-sources Websites/ weblinks)

1. "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" by Dafydd Stuttard and Marcus Pinto.
2. "Metasploit: The Penetration Tester's Guide" by David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni.
3. "Hacking: The Art of Exploitation" by Jon Erickson.
4. "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" by Michael Sikorski and Andrew Honig.
5. "Black Hat Python: Python Programming for Hackers and Pentesters" by Justin Seitz.
6. "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy" by Patrick Engebretson.
7. "The Shellcoder's Handbook: Discovering and Exploiting Security Holes" by Chris Anley, John Heasman, Felix Lindner, and Gerardo Richarte.

TEACHING LEARNING STRATERGIES

- Hands-on-oriented lecturing, collaborative learning, case studies and project presentations, and peer-led discussions.

MODE OF TRANSACTION

- Lecture, seminar, discussion, audio and video presentation, demonstration, practical assignments, and exercises.

ASSESSMENT RUBRICS

Component	Marks
End Semester Evaluation	**60**
Continuous Evaluation	**40**

• Seminar Internal	10
• Case studies / Project(individual)	10
• Assignments	05
• Test	15
Total	**100**

Sample Questions to test Outcomes.

1. What are some common cybersecurity vulnerabilities found in web applications?
2. What are the main objectives of a penetration test?
3. What is the principle of least privilege and why is it important in maintaining cybersecurity?
4. What is the concept of "defense in depth" and how does it enhance an organization's security posture?
5. What are the main objectives of a penetration test?
6. What is wireless phishing, and how can attackers exploit it to trick users into revealing sensitive information on wireless networks?

SEMESTER I
CORE COURSE
PDCS01C05 INFORMATION SECURITY

Course Description

The foundations of information security are thoroughly introduced in this course. The four modules of the course each cover a different topic, including ciphers and secret messages, security attacks and services, block cipher principles, classical encryption techniques, advanced encryption standards, public key cryptography, RSA and other public-key cryptosystems, message authentication, digital signatures, and network security. This course gives students a thorough understanding of the fundamentals of cryptography, security risks, modes of attack, and cryptographic models, as well as practical knowledge of using these concepts in a variety of contexts.

Course Objectives

1. Provide an overview of the fundamental principles, concepts, and components of information security.
2. Understand the importance of security policies, procedures, and governance frameworks in ensuring effective information security management.
3. Provide an in-depth understanding of symmetric key encryption algorithms and their role in securing data.
4. Understand key management practices for AES, including key generation, storage, distribution, and rotation.

Credit			Teaching Hours			Assessment		
L/T	P/I	Total	L/T	P/I	Total	CE	ESE	Total
3	-	3	2	2	3	40	60	100

Lecture/Tutorials, P/I=Practical/Internship, CE =Continuous Evaluation, ESE =End Semester Evaluation.

COURSE OUTCOMES

Course Learning Outcomes: At the end of the Course, the Student will be able to -

C01	Attain knowledge on the basic concepts of cryptography and security.
C02	Understand and design classical encryption techniques and block ciphers.
C03	Familiarize with the block ciphers used in encryption, DES, and AES
C04	Understand and analyze public-key cryptography, RSA and other public-key cryptosystems.
C05	Obtain knowledge about Hashing and SHA algorithm.
C06	Accomplish knowledge about Message Authentication and MAC codes.
C07	Know about digital signatures, digital signature schemes and Digital Signature Standard (DSS).

*Course outcomes based on revised blooms taxonomy

COURSE CONTENTS

Module 1

Foundations of Cryptography and security: Ciphers and secret messages, security attacks and services. Classical Encryption techniques -Symmetric cipher model, substitution techniques, transposition techniques, steganography. Basic Concepts in Number Theory and Finite Fields.

Module 2

Block cipher principles – The data encryption standard (DES) – strength of DES – Differential and linear cryptanalysis – Block cipher design principles. Advanced encryption standard – AES structure – AES transformation function – key expansion – implementation. Block cipher operations –Multiple encryption – ECB – CBC – CFM – OFM – Counter mode. Pseudo Random Number generators - design of stream cipher, RC4.

Module 3

PublicKeycryptography:Primenumbersandtestingfor primality, factoring

largenumbers,discretelogarithms. Principles of public-key crypto systems – RSA algorithm. Diffi-Helman Key exchange, ElgammalCryptographic systems - Hash functions – examples – application – requirements and security – Hash functionbased onCipher block chaining– Secure Hashalgorithm.

Module 4

Message authentication requirements - Message authentication functions – requirements of message authentication codes - MAC security – HMAC – DAA – CCM – GCM. Digital signatures, Digital signature standard. Transport-Level Security,Wireless Network Security, Electronic Mail Security, IP Security.

Core Compulsory Readings (Books, Journals, E-sources Websites/ weblinks)

1. WilliamStallings,CryptographyandNetworkSecurity,Pearson2004
2. FoorouzanandMukhopadhyay,CryptographyandNetworksecurity,2nd edn
3. BuceSchneier.,Appliedcryptography–protocolsandalgorithms,SpringerVerlag2003
4. Williamstallings,NetworkSecurityEssentials,4thedn,Pearson
5. PfleegerandPfleeger,SecurityinComputing,4thEdn,Pearson

Core Suggested Readings (Books, Journals, E-sources Websites/ weblinks)

1. Fundamentals of Information Security: Provide an overview of the fundamental principles, concepts, and components of information security.
2. Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime" by Ralph D".
3. Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom" by Lars E. Daniel and Paul B. House. Clifford.
4. Cyberspace Law: Censorship and Regulation of the Internet" by Hannibal Travis.
5. "Computer Forensics: Cybercriminals, Laws, and Evidence" by Marie-Helen Maras.
6. "Intellectual Property: Patents, Copyrights, Trademarks, and Allied Rights" by W.R. Cornish, David Llewelyn, and Tanya Aplin.

TEACHING LEARNING STRATEGIES

- Hands-on-oriented lecturing, collaborative learning, case studies and project presentations, and peer-led discussions.

MODE OF TRANSACTION

- Lecture, Seminar, Discussion, audio and video presentation, demonstration, practical assignments and exercises.

ASSESSMENT RUBRICS

Component	**Marks**
End Semester Evaluation	**60**
Continuous Evaluation	**40**
• Seminar Internal	10
• Case studies / Project(individual)	10
• Assignments	05
• Test	15
Total	**100**

Sample Questions to test Outcomes.

1.Explain the concepts of confidentiality, integrity, and availability (CIA) in the context of information security.

2.Explain the legal and regulatory requirements that organizations need to comply with regarding information security.

3.Explain the different components of the AES algorithm, including key expansion, substitution, permutation, and mix columns.

4.Discuss the use of AES in different applications and industries, such as financial transactions, cloud computing, and IoT devices.

5.Explain the principles of public-key cryptography and how it is used for data encryption and decryption.

SEMESTER II
ELECTIVE COURSE
PDCS02E01 Security Auditing

Course Description

The Security Auditing course offers a thorough introduction to the establishment and maintenance of audit functions. Attendees will acquire the skills to audit operating systems, web servers, applications, databases, and storage options. Furthermore, they will develop proficiency in auditing network devices. The course also addresses the application of standards and frameworks like COBIT, ITIL, and ISO while providing an understanding of regulations such as Sarbanes-Oxley, HIPAA, and PCI. Ultimately, this course equips participants with the essential knowledge and capabilities to conduct efficient IT audits within any organization.

Course Objectives

- Provide an overview of security auditing, its importance, and its role in identifying vulnerabilities and risks in systems and networks.
- Introduce different methodologies and frameworks for conducting security audits, such as ISO/IEC 27001, NIST Cybersecurity Framework, and CIS Controls.
- Familiarize with the process of establishing security baselines for network devices and conducting audits to ensure compliance with the established standards.
- Introduction to Application Standards and Frameworks: Provide an overview of different application standards and frameworks, such as OWASP Top 10, PCI DSS, HIPAA, and ISO/IEC 27001.
- Cover techniques for auditing web applications, including identifying common vulnerabilities, analyzing input validation and output encoding, and assessing session management.

Credit			Teaching Hours			Assessment		
L/T	P/I	Total	L/T	P/I	Total	CE	ESE	Total
4	-	4	2	2	4	40	60	100

Lecture/Tutorials, P/I=Practical/Internship, CE =Continuous Evaluation, ESE =End Semester Evaluation

COURSE OUTCOMES

Course Learning Outcomes: At the end of the Course, the Student will be able to -

C01	Build and maintain an internal IT audit function that meets industry standards and best practices.
C02	Audit operating systems, web servers, applications, databases, and storage solutions to identify and mitigate control weaknesses.
C03	Check for vulnerabilities in switches, routers, and firewalls, and be able to audit virtualized environments for security.
C04	Understand regulations - Sarbanes-Oxley, HIPAA, and PCI to implement risk management techniques.
C05	Use standards and frameworks, such as COBIT, ITIL, and ISO, to guide IT audit activities and ensure compliance with industry standards.

*Course outcomes based on revised blooms taxonomy

COURSE CONTENTS

Module 1

Basics of IT Auditing

Build and maintain an internal IT audit function with maximum effectiveness and value Audit entity-level controls and cybersecurity programs-Assess data centers and disaster recovery.

Module 2

OS- Application Auditing

Evaluate Windows, UNIX, and Linux operating systems-Audit Web servers and applications-Analyze databases and storage solutions-Review big data and data repositories-Assess end user computer devices, including PCs and mobile devices.

Module 3

Device auditing

Examine switches, routers, and firewalls- Audit virtualized environments-Evaluate risks associated with cloud computing and outsourced operations-Drill down into applications and projects to find potential control weaknesses Learn best practices for auditing new technologies.

Module 4

Standards

Usestandards and frameworks, such as COBIT, ITIL, and ISO Understand regulations, including Sarbanes-Oxley, HIPAA, and PCI Implement proven risk management practices.

Core Compulsory Readings (Books, Journals, E-sources Websites/ weblinks)

1. IT audit Control and Security by Robert R Moeller.
2. Standard for Auditing Computer Applications by Martin Krist.
3. Security and Auditing of Smart Devices by SajayRai , Philip Chukwuma , Richard Cozart.

Core Suggested Readings (Books, Journals, E-sources Websites/ weblinks)

1. "The Basics of IT Audit: Purposes, Processes, and Practical Information" by Stephen D. Gantz.
2. "Auditing IT Infrastructures for Compliance" by Martin Weiss.
3. "Auditing Network Security" by Chris Jackson and Steve Mansfield-Devine.

4. "Auditing and Security: AS/400, NT, UNIX, Networks, and Disaster Recovery Plans" by Ivan G. Guardiola.
5. "ISO 27001/ISO 27002: A Pocket Guide" by Alan Calder.

TEACHING LEARNING STRATEGIES

- Hands-on-oriented lecturing, collaborative learning, case studies and project presentations, and peer-led discussions.

MODE OF TRANSACTION

- Lecture, seminar, discussion, audio and video presentation, demonstration, practical assignments, and exercises.

ASSESSMENT RUBRICS

Component	**Marks**
End Semester Evaluation	**60**
Continuous Evaluation	**40**
• Seminar Internal	10
• Case studies / Project(individual)	10
• Assignments	05
• Test	15
Total	**100**

<u>Sample Questions to test Outcomes.</u>

1. What is the purpose of security auditing, and why is it important for organizations to conduct regular security audits?

2. What are some common security controls and practices that are typically assessed during a security audit?

3. Discuss the role of compliance frameworks, such as ISO 27001 and NIST Cybersecurity Framework, in guiding security audits.

4. What are some common vulnerabilities and risks associated with network devices, and how can they be mitigated?

5.Discuss the role of configuration management and change control in network device auditing.

6.Discuss the importance of complying with industry-specific application standards and regulations, such as PCI DSS, HIPAA, or GDPR.

SEMESTER II
ELECTIVE COURSE
PDCS02E02 Cyber Law and IT Act

Course Description

This course examines numerous facets of cyber law and the Information Technology Act in India, as well as various cyber-crimes and intellectual property rights. It offers fundamental knowledge of cyberspace, encompassing topics such as e-governance and e-commerce. Furthermore, the course delves into the objectives of cybercrimes, including cyber stalking, cyber terrorism, and social networking offenses. The Information Technology Act of 2000 is discussed in detail, covering its development, key features, and regulatory framework, as well as pertinent intellectual property rights, patents, and copyright laws associated with the internet.

Course Objectives

- Understanding Cyber Crimes: Provide an overview of cyber-crimes, their types, and their impact on individuals, organizations, and society.
- Understanding the practices in securing personal and organizational information, protecting against cyber-attacks, and fostering a culture of cyber security.
- Explore the provisions of the IT Act related to electronic contracts, digital signatures, and legal aspects of e-commerce transactions.
- Develop skills and strategies for responding to and mitigating cyber terrorism incidents, including coordination with law enforcement and intelligence agencies.

Credit			**Teaching Hours**			**Assessment**		
L/T	P/I	Total	L/T	P/I	Total	CE	ESE	Total
4	-	4	2	2	4	40	60	100

Lecture/Tutorials, P/I=Practical/Internship, CE =Continuous Evaluation, ESE =End Semester Evaluation

COURSE OUTCOMES

Course Learning Outcomes: At the end of the Course, the Student will be able to -

C01	Understand the fundamentals of cyber law and cyber space and the scope of Cyber Law.
C02	Develop an understanding of the problems relating to e-commerce transactions.
C03	Know the various aspects of cybercrimes - cyber stalking, pornography, forgery, fraud, bullying, virtual crimes, email bombing, keyloggers, murder, and social networking crimes.
C04	Analyze Section 66A, 66B, 66C, 66D, 66E, 69A, and 69B of IT Act 2000.
C05	Get an extensive knowledge regarding IT Act 2000 need for IT act.
C06	Understand various authorities under the IT Act and their powers and the regulatory framework of the IT Act 2000.
C07	Distinguish and explain various forms of IPRs.
C08	Analyze rights and responsibilities of holder of Patent, Copyright, Authorship etc.

*Course outcomes based on revised blooms taxonomy

COURSE CONTENTS

Module 1

Cyberspace & Cyber Law

Cyber Space- Fundamental definitions, Jurisdiction in Cyber Space - Indian Context of Jurisdiction, Enforcement agencies, Need for IT act, Scope of Cyber laws,IPRS, E-governance, E-commerce & legal aspects-Types of e-commerce, Legal aspects of e-commerce, E–commerce and laws in India, E-contracts-Types of e-contracts, Online identity, Digital signature, Things to secure a system, Authentication- PKI Authentication,Inter-operable technology standards, Privacy & Data protection, Cyber law in India with Special reference to IT Act, 2000.

Module 2

Cyber Crimes

Cybercrimes and their objectives, Kinds of cybercrime –Cyber stalking, Cyber pornography, Forgery and Fraud, Virtual crimes, Theft of computer source code, Email bombing, Keyloggers, Cyber murder, Social networking crime, Cyber bullying, Section - 66A,66B,66C,66D,66E,69A,69B. Cyber terrorism, Mobile crimes and cases, Crime related to IPRS, Data privacy &confidentiality, Freedom of speech, Reasons for commission of cyber-crime, cyber forensic.

Module 3

The Information Technology Act 2000

Evolution of the IT Act, Genesis and Necessity, Salient features of the IT Act, 2000,IPC,E-courts,Various authorities under IT Act and their powers, Regulatory Framework of IT Act 2000 - Digital Signature, E-Signature, Electronic Records, Electronic Evidence and Electronic Governance. Penalties & Offences, Impact on other related Acts (Amendments) - Amendments to Indian Penal Code, Amendments to Indian Evidence Act, Amendments to Bankers Book Evidence Act, Amendments to Reserve Bank of India Act.

Module 4

Intellectual Property Rights

Different acts governing IPR,various forms of IP,cyber space players,patents- authorship and assignment issues - copyright in internet - multimedia and copyright issues,software piracy -. intellectual property rights, sensitive personal data or information under section 43A-IT act,Domain name disputes, jurisdiction, extraterritorial provision,Liability- types of liabilities, evidence aspects, taxation, UNCITRAL model law on e-commerce, key aspects of model law- non-discrimination.

Core Compulsory Readings (Books, Journals, E-sources Websites/ weblinks)

1. Textbook on Cyber Law by Duggal Pavan
2. An Introduction to CYBER LAW by DR JP Mishra Edition 2014

3. Cyber Laws & Cyber Crimes by Dr. Santhosh Kumar
4. Commentary on The Information Technology Act by Vijay K. Sondhi Edition 2022
5. Supreme Court on Intellectual Property by Surendra Malik and Sudeep Malik
6. Law Relating to Intellectual Property Rights by VK AHUJA Edition 2020

Core Suggested Readings (Books, Journals, E-sources Websites/ weblinks)

1. "Cybercrime and Digital Investigation: An Introduction" by Ian Walden.
2. "Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes" by Albert Marcella Jr. and Doug Menendez.
3. "The Dark Net: Inside the Digital Underworld" by Jamie Bartlett.
4. Handbook of Digital Forensics and Investigation" by Eoghan Casey.
5. "Intellectual Property Rights in the Global Economy" by Keith E. Maskus.

TEACHING LEARNING STRATEGIES

- Hands-on-oriented lecturing, collaborative learning, case studies and project presentations, and peer-led discussions.

MODE OF TRANSACTION

- Lecture, seminar, discussion, audio and video presentation, demonstration, practical assignments, and exercises.

ASSESSMENT RUBRICS

Component	**Marks**
End Semester Evaluation	**60**
Continuous Evaluation	**40**
• Seminar Internal	10
• Case studies / Project(individual)	10
• Assignments	05
• Test	15

Total	**100**

Sample Questions to test Outcomes.

1. What are the key legal frameworks and regulations governing cyberspace at the national and international levels?

2. What are the legal implications of cyber activities such as hacking, data breaches, and online fraud?

3.How does cyber law address issues related to privacy, data protection, and digital rights?

4.What are the emerging legal challenges and issues in the field of cyber-crime and digital technology?

5.What are the different types of Intellectual Property Rights, such as copyrights, patents, trademarks, and trade secret?

6. How does Intellectual Property law differ from country to country, and what are the international agreements that govern IP rights?

SEMESTER II
ELECTIVE COURSE
PDCS02E03 BLOCKCHAIN AND CRYPTOCURRENCY TECHNOLOGIES

Course Description

The goal of this course is to familiarize students with the functional/operational features of the Bitcoin ecosystem as well as Blockchain Technology. It delves into the fundamentals of cryptocurrency and cryptography. In the course, blockchain technology is also covered. Cryptocurrency, bitcoin, is covered in detail, about the workings of bitcoin, bitcoin mining, and the community, politics, and legal framework that surround cryptocurrency. Overall, the course provides a thorough grasp of cryptography and cryptocurrencies, including its technical foundations, practical applications, and social impacts.

Course Objectives

- Understand different blockchain architectures, consensus algorithms, and their implications for security, scalability, and decentralization.
- Understand emerging trends in blockchain technology, such as blockchain interoperability, scalability solutions, and the impact of emerging technologies like AI and IoT.
- Provide an overview of the history, concepts, and features of cryptocurrencies, with a specific focus on Bitcoin.
- Explain the process of cryptocurrency mining, including the consensus algorithms, mining hardware, and the environmental impact.

Credit			**Teaching Hours**			**Assessment**		
L/T	P/I	Total	L/T	P/I	Total	CE	ESE	Total
4	-	4	2	2	4	40	60	100

Lecture/Tutorials, P/I=Practical/Internship, CE =Continuous Evaluation, ESE =End Semester Evaluation

COURSE OUTCOMES

Course Learning Outcomes: At the end of the Course, the Student will be able to -

C01	Know the cryptographic fundamentals required to comprehend cryptocurrencies.
C02	explain how blockchain works and develop strong technical understanding of Blockchain.
C03	Discover how the transactions, script, and blocks parts of the Bitcoin protocol work together to create the entire system.
C04	Understand how Bitcoins works when utilizing.
C05	Explain the process of Bitcoin mining.
C06	Know the role of anonymity and privacy in Bitcoin ecosystem.
C07	Recognize how the Bitcoin consensus works and how blockchain technologies are used in real-world settings.

*Course outcomes based on revised blooms taxonomy

COURSE CONTENTS

Module 1

Introduction to Cryptography and Cryptocurrencies: Foundations of Cryptography and security: Ciphers and secret messages, security attacks and services. Mathematical tools for cryptography: substitution techniques, modular arithmetic, Euclid's algorithm, finite fields, polynomial arithmetic. Design Principles of Block Ciphers: Theory of Block Cipher Design, Feistel cipher network structure, DES and Triple DES, modes of operation (ECB, CBC, OFB, CFB), strength of DES.

Module 2

Blockchain Achieves:Decentralization-Centralization vs. Decentralization-Distributed consensus, Consensus with- out identity using a blockchain, Incentives and proof of work.

Simple Local Storage, Hot and Cold Storage, Splitting and Sharing Keys, Online Wallets and Exchanges, Payment Services,Transaction Fees, Currency Exchange Markets.

Module 3

Mechanics of Bitcoin: Bitcoin transactions, Bitcoin Scripts, Applications of Bitcoin scripts, Bitcoin blocks, The Bit- coin network, Limitations, and improvements. Bitcoin Mining: The task of Bitcoin miners, Mining Hardware, Energy consumption and ecology, Mining pools, Mining incentives and strategies. Bitcoin and Anonymity: Anonymity Basics, How to De-anonymize Bitcoin, Mixing, Decentralized Mixing, Zero coin and Zero cash.

Module 4

Community, Politics, and Regulation: Consensus in Bitcoin, Bitcoin Core Software, Stakeholders: Who's in Charge, Roots of Bitcoin, Governments Notice on Bitcoin, Anti Money Laundering Regulation, New York's Bit License Proposal. Bitcoin as a Platform: Bitcoin as an Append only Log, Bitcoin as Smart Property, Secure Multi Party Lotteries in Bitcoin, Bitcoin as Public Randomness, Source-Prediction, Markets, and Real-World Data Feeds.

Core Compulsory Readings (Books, Journals, E-sources Websites/ weblinks)

1. Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. (2016).
2. William Stallings, Cryptography and Network Security, Pearson2004.
3. Antonopoulos, A. M. (2014). Mastering Bitcoin: unlocking digital cryptocurrencies.OReillyMedia, Inc.".
4. Franco, P. (2014). Understanding Bitcoin: Cryptography, engineering and economics. JohnWileyandSons.

Core Suggested Readings (Books, Journals, E-sources Websites/ weblinks)

1. "Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications" by Imran Bashir.
2. "Blockchain: The Insights You Need from Harvard Business Review" by Harvard Business Review.

3. "Blockchain for Dummies" by Tiana Laurence.
4. Cryptocurrency: How Bitcoin and Digital Money are Challenging the Global Economic Order" by Antony Lewis.
5. "The Bitcoin Standard: The Decentralized Alternative to Central Banking" by Saifedean Ammous.
6. "The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order" by Paul Vigna and Michael J. Casey.

TEACHING LEARNING STRATEGIES

- Hands-on-oriented lecturing, collaborative learning, case studies and project presentations, and peer-led discussions.

MODE OF TRANSACTION

- Lecture, seminar, discussion, audio and video presentation, demonstration, practical assignments, and exercises.

ASSESSMENT RUBRICS

Component	**Marks**
End Semester Evaluation	**60**
Continuous Evaluation	**40**
• Seminar Internal	10
• Case studies / Project(individual)	10
• Assignments	05
• Test	15
Total	**100**

Sample Questions to test Outcomes.

1. What are the key features and benefits of blockchain technology?

2. What are the different types of blockchains (public, private, consortium) and their use cases?

3. How does the Bitcoin network achieve consensus and validate transactions?

4. What are the potential risks and security considerations in blockchain implementation?

5. What are the security measures in place to protect Bitcoin wallets and transactions?

6. How do cryptocurrencies handle issues such as double-spending and transaction validation?

SEMESTER II
ELECTIVE COURSE
PDCS01E04Cyber Forensic

Course Description

The focus of the course is on various aspects of cyber forensics. This course offers an in-depth understanding of computer forensics fundamentals and the methodology for conducting forensic investigations, as well as the applicable forensic tools. Furthermore, the course addresses the collection, storage, and management of forensic data, along with significant hardware and software tools required. It also encompasses techniques for analyzing and validating forensic data. Additionally, the course demonstrates real-world applications of digital forensics through the utilization of essential tools.

Course Objectives

- Provide an overview of digital forensics, its importance in investigating cybercrime, and its role in legal proceedings.
- Teach proper techniques for collecting and preserving digital evidence in a forensically sound manner, ensuring its admissibility in court.
- Familiarize with commonly used digital forensic tools and software for acquiring, analyzing, and reporting on digital evidence.
- Cover techniques for examining volatile memory to identify running processes, extract artifacts, and discover evidence of malicious activities.

Credit			Teaching Hours			Assessment		
L/T	P/I	Total	L/T	P/I	Total	CE	ESE	Total
4	-	4	2	2	4	40	60	100

Lecture/Tutorials, P/I=Practical/Internship, CE =Continuous Evaluation, ESE =End Semester Evaluation

COURSE OUTCOMES

Course Learning Outcomes: At the end of the Course, the Student will be able to -

C01	Understand fundamentals of cyber forensic, learn investigation tools and techniques, analysis of data to identify evidence.
C02	Explain how to conduct a digital forensics investigation and how to report findings from digital forensic investigations using various forensic tools.
C03	Accomplish the knowledge about Computer Forensics analysis and validation techniques.
C04	Perform recovery of digital evidence from various digital devices using a variety of software utilities.
C05	Know about cloud forensics and IoT forensics.

*Course outcomes based on revised blooms taxonomy

COURSE CONTENTS

Module 1

Computer Forensics and Investigation

Understanding computer forensics-Preparing for Computer Investigations-Corporate High-Tech Investigation-Data Acquisition and Recovery-Storage Formats-Using acquisition tools-Data Recovery-RAID Data acquisition.

Module 2

Processing Crime and Incident Scene

Identifying and collecting evidence-Preparation for search, Seizing and Storing Digital evidence. Computer Forensics tools (Encase)-Windows Operating System-Understanding file structure and file system-NTFS disks-Disk Encryption-Registry-Evidence Manipulation-Computer Forensics software and hardware tools-Chain of Custody-Handling digital evidence – best practices.

Module 3

Computer Forensics Analysis and Validation

Data collection and analysis-Validation of forensics data-Data hiding technique-Email Investigation and Mobile device Forensics-Investigation of e-mail crimes and Violations-Using specialized E-mail forensics tools-Understanding mobile device forensics and Acquisition procedures.

Module 4

Role of Digital Forensics in Real time applications

SANS SIFT Investigative tool-PRO Discover Basic-Volatility-Sleuth Kit-CAINE investigative environment Industry Trends-Forensics Standards-Introduction to Cloud Forensics-Introduction to IoT Forensics.

Core Compulsory Readings (Books, Journals, E-sources Websites/ weblinks)

1. Bill Nelson, Amelia Philips, Christopher Steuart, Guide to Computer Forensics and Investigations, Fourth Edition, Cengage Learning, 2016.
2. David Lilburn Watson, Andrew Jones, Digital Forensics Processing and Procedures, Syngress, 2013.
3. Cory Altheide, Harlan Carvey, Digital Forensics with Open-Source Tools, British Library Cataloguing-in-Publication Data, 2011
4. Greg Gogolin, Digital Forensics Explained Press, 2013.

Core Suggested Readings (Books, Journals, E-sources Websites/ weblinks)

1. "Digital Forensics with Open-Source Tools" by Cory Altheide and Harlan Carvey.
2. "Computer Forensics: Investigating Network Intrusions and Cyber Crime" by EC-Council.
3. "File System Forensic Analysis" by Brian Carrier.
4. "Practical Mobile Forensics" by Heather Mahalik, Rohit Tamma, and Satish Bommisetty.
5. "Digital Forensics: Threatscape and Best Practices" by John Sammons.

TEACHING LEARNING STRATEGIES

- Hands-on Oriented Lecturing, Collaborative Learning, Case Studies and Project Presentations, Peer-Led Discussions.

MODE OF TRANSACTION

- Lecture, seminar, discussion, audio and video presentation, demonstration, practical assignments, and exercises.

ASSESSMENT RUBRICS

Component	Marks
End Semester Evaluation	**60**
Continuous Evaluation	**40**
• Seminar Internal	10
• Case studies / Project(individual)	10
• Assignments	05
• Test	15
Total	**100**

Sample Questions to test Outcomes.

1. What are the key differences between traditional forensics and cyber forensics?

2. Explain the steps involved in conducting a cyber forensics investigation.

3. What are the key techniques and tools used in cyber forensics?

4. What is digital forensics, and what types of evidence can be obtained in a digital forensics' investigation?

5. What are the different types of digital evidence encountered in digital forensics investigations?

SEMESTER II
ELECTIVE COURSE
PDCS02E05 BIOMETRIC IMAGE PROCESSING

Course Description

The course thoroughly examines image-based biometric systems, which primarily focuses on processing human biometric traits including the hand, iris, and face using image processing methods. It imparts essential knowledge on digital image processing, image sensing, and acquisition. Additionally, the course investigates spatial and frequency domain image enhancement techniques, several image segmentation methods, and morphological image processing concepts. The course addresses face, hand, and iris biometrics by discussing 2D and 3D facial recognition techniques and preprocessing and feature extraction from hand and iris biometric imagery. Lastly, an overview of fusion in biometrics is provided.

Course Objectives

- Provide an overview of biometric systems, their applications, and the principles behind biometric authentication.
- Discuss the ethical and legal implications of biometric systems, including privacy concerns, data protection, and compliance with regulations.
- Examine advanced topics in image processing, such as image understanding, object recognition, scene analysis, and machine learning-based approaches.
- Explore the application areas of digital image processing, such as medical imaging, remote sensing, surveillance, and multimedia.

Credit			**Teaching Hours**			**Assessment**		
L/T	P/I	Total	L/T	P/I	Total	CE	ESE	Total

4	-	4	2	2	4	40	60	100

Lecture/Tutorials, P/I=Practical/Internship, CE =Continuous Evaluation, ESE =End Semester Evaluation

COURSE OUTCOMES

Course Learning Outcomes: At the end of the Course, the Student will be able to -

C01	Familiarize the fundamentals of a digital image processing system.
C02	Perform image transformation using Fourier transform and discrete cosine transform.
C03	To perform image enhancement like gray level transformations, smoothing and sharpening images using spatial and frequency-based methods, edge detection in images, image thresholding.
C04	Apply morphological operations such as dilation and erosion, compound operations, and morphological filtering to process images.
C05	Perform 2D and 3D face recognition using Global, local and hybrid techniques.
C06	Perform minutiae point extraction from fingerprint images for fingerprint recognition.
C07	Understand and implement main steps of an iris recognition system - image acquisition, segmentation, normalization, encoding and matching.
C08	Gain knowledge about Multibiometric systems and how it utilizes the principle of fusion and various levels of fusion.

*Course outcomes based on revised blooms taxonomy.

COURSE CONTENTS

Module 1

Digital image representation, Fundamental steps in image processing, Elements of digital image processing system, Image sensing and acquisition, Sampling and quantization, Basic relationship between pixels, Transformation technology: Fourier transform - Discrete cosine transform.

Module 2

Image enhancement: Spatial domain methods: Basic grey level transformations - Histogram equalization - Smoothing spatial filter - Sharpening spatial filters - Laplacian, Frequency domain methods: Smoothing and sharpening filters – Ideal - Butterworth - Gaussian filters. Image Segmentation: Point- Line and edge detection - Thresholding - Global and multiple thresholding, Region splitting and merging.

Module 3

Morphological image processing: Fundamental concepts and operations, Dilation and Erosion, Compoundoperations, Morphological filtering, Basic morphological algorithms, Grayscale morphology. 2D and 3D facebiometrics: Global face recognition techniques: Principal component analysis - Face recognition using PCA -Linear discriminant analysis- Face recognition using LDA, Local face recognition techniques: GeometricTechniques-
Elasticgraphmatchingtechniques,Hybridfacerecognitiontechniques.3DFaceImage:Acquisition,Pre-processingandnormalization,3D face.

Module 4

Hand and Iris Biometrics: Characterization by minutiae extraction: Histogram equalization, Binarization, Skeletonization, Detection of minutiae, Matching, Performance evaluation, preprocessing of iris images: Extraction of region of interest - Construction of noise mask – Normalization - Features extraction and encoding - Similarity measures between two iris codes. Fusion in biometrics: Multi-biometrics, Levels of fusion: Sensor level - Feature level - Rank level - Decision level fusion - Score level fusion.

Core Compulsory Readings (Books, Journals, E-sources Websites/ weblinks)

1. RafaelCGonzalez,RichardEWoodsandStevenLEddins,“DigitalImageProcessing”,PearsonEducation,NewDelhi,2013.
2. AmineNaitAliandRegisFournier,“SignalandImageProcessingfor Biometrics”,JohnWileyandSons,UK,2012.

3. ArunARoss,KarthikNandakumarandJainAK,“HandbookofMulti-biometrics”,Springer,NewDelhi2011.
4. OgeMarques,“PracticalImageandVideoProcessingusingMATLAB”,JohnWileyandSons,NewJersey,2011.

Core Suggested Readings (Books, Journals, E-sources Websites/ weblinks)

1. "Biometrics: Concepts, Methodologies, Tools, and Applications" edited by Constantinos Pattichis.
2. "Handbook of Biometrics" edited by Anil K. Jain, Ruud M. Bolle, and Sharath Pankanti.
3. "Digital Image Processing" by Rafael C. Gonzalez and Richard E. Woods.
4. "Digital Image Processing: Concepts, Algorithms, and Scientific Applications" by Bernd Jähne.
5. "Fundamentals of Digital Image Processing" by Chris Solomon and Toby Breckon.

TEACHING LEARNING STRATEGIES

- Hands-on-oriented lecturing, collaborative learning, case studies and project presentations, and peer-led discussions.

MODE OF TRANSACTION

- Lecture, seminar, discussion, audio and video presentation, demonstration, practical assignments, and exercises.

ASSESSMENT RUBRICS

Component	Marks
End Semester Evaluation	**60**
Continuous Evaluation	**40**
• Seminar Internal	10
• Case studies / Project(individual)	10

• Assignments	05
• Test	15
Total	**100**

Sample Questions to test Outcomes.

1. Discuss the advantages and limitations of different biometric modalities such as fingerprint, face, iris, voice, and palmprint.
2. How can biometric systems be integrated into various applications, such as access control, identity verification, and forensic investigations?
3. What is digital image processing and why is it important in various fields, such as medicine, remote sensing, and multimedia?
4. Discuss emerging trends in biometric systems, such as behavioral biometrics, mobile biometrics, and continuous authentication.
5. Explain the concept of image segmentation and various algorithms used for partitioning images into meaningful regions.
6. Describe techniques for image registration and alignment, such as point-based and intensity-based registration.

SEMESTER II
ELECTIVE COURSE
PDCS02E06 SPEECH, AUDIO AND VIDEO FORENSICS

Course Description

This course examines the utilization of speech, linguistics, and media within forensic science, concentrating on the fundamentals of sound, analysis and synthesis of sound and speech, as well as electronic recording and transmission devices. Furthermore, it delves into forensic linguistics, investigating a range of linguistic methodologies and various techniques applied in this field. The course also emphasizes the methods and best practices employed for forensic speaker identification, in addition to audio and video forensic evaluations.

Course Objectives

- Provide an overview of the field of forensic linguistics and its applications in legal and forensic contexts.
- Explore methods for analyzing speech patterns and vocal characteristics to determine speaker identity and authenticity.
- Study techniques for analyzing and authenticating digital media, including audio and video recordings, images, and text messages.
- Discuss the ethical and legal implications of utilizing speech, linguistics, audio, video and media in forensic science.

Credit			**Teaching Hours**			**Assessment**		
L/T	P/I	Total	L/T	P/I	Total	CE	ESE	Total
4	-	4	2	2	4	40	60	100

Lecture/Tutorials, P/I=Practical/Internship, CE =Continuous Evaluation, ESE =End Semester Evaluation

COURSE OUTCOMES

Course Learning Outcomes: At the end of the Course, the Student will be able to -

C01	Understand the basic principles of voice and the physics involved in sound production.
C02	Identify and explain various audio and video technologies, playback devices, storage options, and preservation techniques.
C03	Recognize the significance of language-related evidence in court.
C04	Distinguish the many linguistic data types that might be cited as proof.
C05	Utilize various strategies and approaches to identify and recognize speakers in forensic situations following the concept of test and error. in speaker identification.
C06	Convert various speech file formats into forensic voice module formats and gain knowledge about different types of spectrograms and how they are used in forensic analysis.
C07	Understand how to extract and analyze video files from storage media andhow to validate the presence of metadata in the video or audio files.

*Course outcomes based on revised blooms taxonomy

COURSE CONTENTS

Module 1

Physics of sound: waves and sound, analysis and synthesis of complex waves, Human and non-human utterances, anatomy of vocal tract, vocal formants, analysis of vocal sound, frequencies, andovertones.ElectronicsofAudioRecording,TransmissionandPlaybackdevices, noise and distortion, voice storage and preservation.

Module 2

ForensicLinguistics:Phonetics,Morphology,Syntax,Semantics,Stylistics,Pragmatics,Script,orthographyandgraphology,Differencebetweenlanguageandspeech,Psycholinguistics,Neurolinguistics, Sociolinguistics, Scientific approaches; Reliability and

admissibility of evidence in the court,linguisticprofile,languageregister. Discourse Analysis:Connivance,acceptance, listening feedback and rejection in the context of MensRea,Narrative,Dialectology,Linguistic variety as age O graphicalmarker,

Idiolectsandspeakercharacterization,Phonology,MorphologyandWordformationproce ssesasindividuallinguisticabilities.

Module 3

Various approaches in Forensic Speaker Identification, Instrumental Analysis of speech sample,Interpretation of result, Statistical interpretation of probability scale, Objective/Subjective methods,discriminating tests, closed test, open test, likelihood ratio calculation, Concept of test and error inSpeakerIdentification, case studies. Techniques and Best Practices for examination of Audio recording authentication and casestudies.

Module 4

Audio /video forensics: Spectrographic – Conversion of different voice file formats into

forensicvoicemoduleformats.Varioustypesofspectrograms,spectrographiccuesforvow elsandconsonants.Speechanalysis in forensicsciences.Speechsynthesis by analysis, Speech recognitionand speaker identification. Fundamentals of Digital Signal processing and communication system.Analogue and digital systems, Analogue signal and digital signals, Analogue to digital and digital toanalogue converters, need and advantages of digital systems and digital signal processing. ForensicextractionofvideofilesfromDVRandotherstoragemedia.Forensicexamination ofDVRcontaining video footages, its frame analysis. Forensic examination and authentication of meta datapresentinvideo/audiofiles.Enhancementofvideo/Photo anditscomparison/authentication.

Core Compulsory Readings (Books, Journals, E-sources Websites/ weblinks)

1. Bengold&NelsonMoryson;“SpeechandAudiosignalprocessing”,JohnWiley&

Sons,USA(1999).

2.D.B.Fry; “The PhysicsofSpeech,Cambridge UniversityPress”,(2004).

3. Dwight Bolingeret. al.; “Aspects of Language”, Third Edition, Harcourt

Brace Jovanovich CollegePublishers, USA, (1981).

4.GloriaJ.Bordenet.al.;“SpeechSciencePrimer(Physiology,Acousticsand

5. PerceptionofSpeech)”,6thEd, aWoltersKluwer Company, USA, (2011).

6. HarryHollien;“ForensicVoiceIdentification”,AcademicPress,London.(2001)

7. HarryHollien;“TheAcousticsofCrimeTheNewScienceofForensic

Phonetics”,PlenumPress,NewYorkand London (1990).

8.OscarTosi;“VoiceIdentificationTheoryofLegalApplications”,

UniversityParkPress,Baltimore (1979).

9.O'Shaughnessy,Douglas;“SpeechCommunication”,HyderabadUniversities

Press(India)Pvt.Ltd. (2001).

10.PatriciaAshby;“SpeechSounds”,2ndEd.Routledge,LondonandNewYork(2005).

11.PhilipRose;“ForensicSpeakerIdentification,”TaylorandFrancis,Forensic

ScienceSeries,London (2002).

12.SimonJ.Godsill;“DigitalAudioRestoration”,Springer,(1998).

Core Suggested Readings (Books, Journals, E-sources Websites/ weblinks)

1. "Forensic Linguistics: An Introduction to Language, Crime, and the Law" by John Olsson.
2. "The Routledge Handbook of Forensic Linguistics" edited by Malcolm Coulthard and Alison Johnson.
3. Forensic Examination of Digital Evidence: A Guide for Law Enforcement" by Andrew Jones and Craig Valli.
4. Forensic Spectroscopy: Methods and Applications" edited by Nicolo Omenetto and Alberto Amadasi.
5. "Spectroscopy for the Biological Sciences" by Gordon G. Hammes.

TEACHING LEARNING STRATEGIES

- Hands-on-oriented lecturing, collaborative learning, case studies and project presentations, and peer-led discussions.

MODE OF TRANSACTION

- Lecture, seminar, discussion, audio and video presentation, demonstration, practical assignments, and exercises.

ASSESSMENT RUBRICS

Component	**Marks**
End Semester Evaluation	**60**
Continuous Evaluation	**40**
• Seminar Internal	10
• Case studies / Project(individual)	10
• Assignments	05
• Test	15
Total	**100**

<u>Sample Questions to test Outcomes</u>.

1.What is forensic linguistics and how does it contribute to criminal investigations and legal proceedings?

2.How can linguistic analysis help identify deception, false statements, or hidden meanings in legal texts and transcripts?

3.How can forensic linguistics assist in identifying and analyzing hate speech, threats, or extremist language?

4. How does digital media analysis contribute to forensic investigations, such as analyzing audio and video recordings or images?

5.Discuss the advancements and challenges in multimedia forensics, including video enhancement or image super-resolution.

6.Discuss the principles and techniques of spectrographic for identifying and analyzing different types of materials.

SEMESTER II
ELECTIVE COURSE
PDCS02E07MACHINE LEARNING FOR CYBER SECURITY

Course Description

This Course focuses on the application of machine learning techniques and algorithms to enhance the security of computer systems and networks. It involves the use of computational models that can automatically learn and make predictions or decisions based on patterns and insights extracted from large amounts of data. In the context of cybersecurity, machine learning algorithms can be trained on various types of data, including network traffic, system logs, malware samples, and user behavior, among others. By analyzing these datasets, machine learning models can identify patterns and anomalies that may indicate potential security threats or vulnerabilities. The course content includes the fundamentals of machine learning, Malware detection, Intrusion detection and prevention, Penetration Testing, Hacking – Password cracking.

Course Objectives

- Understand the applications of Machine learning for Cyber Security
- Explore various machine learning algorithms for implementing the cyber security methods
- Machine learning for Malware analysis and Malware detection.
- Understand the use of machine learning based techniques for social engineering and social networking threats and security features.
- Assess password security and cracking.

Credit	Teaching Hours	Assessment

L/T	P/I	Total	L/T	P/I	Total	CE	ESE	Total
4	-	4	2	2	4	40	60	100

Lecture/Tutorials, P/I=Practical/Internship, CE =Continuous Evaluation, ESE = End Semester Evaluation

COURSE OUTCOMES

Course Learning Outcomes: At the end of the Course, the Student will be able to -

C01	Understand various machine learning techniques suitable for cyber security related problems
C02	Understand Malware and identify the role of machine leaning for detecting malwares
C03	Identify various threats in social networking. Role of machine learning for social network analysis
C04	Understand penetration testing and how it will be useful for identifying the threats in web-based systems.
C05	Understanding Intrusion detection and Prevention systems.
C06	Importance of machine learning for intrusion prevention and detection system.
C07	Assess password security and various vulnerabilities associated with passwords

*Course outcomes based on revised blooms taxonomy

COURSE CONTENTS

Module1

Machine Learning for Cybersecurity: Train-test-splitting your data, standardizing your data, Summarizing large data using principal component analysis, Generating text using Markov chains, Performing clustering using scikit-learn, Training an XGBoost classifier, Analyzing time series using statsmodels, Anomaly detection with Isolation Forest, Natural language processing using a hashing vectorizer and tf-idf with scikit-learn, Hyperparameter tuning with scikit-optimize

Module 2

Machine Learning-Based Malware Detection: Malware static analysis, Malwaredynamic analysis,, Using machine learning to detect the file type, Measuring the similarity between two strings, Measuring the similarity between two files, Extracting N-grams, Selecting the best N-grams, Building a static malware detector, Tackling class imbalance. Handling type I and type II errors. Machine Learning for Social Engineering: Twitter spear phishing bot, Voice impersonation, Speech recognition for OSINT, Facial recognition, Deepfake, Deepfake recognition, Lie detection using machine learning, Personality analysis, Social Mapper, Fake review generator, Fake news

Module 3

Penetration Testing Using Machine Learning:, CAPTCHA breaker, Neural network-assisted fuzzing, DeepExploit, Web server vulnerability scanner using machine learning (GyoiThon), Deanonymizing Tor using machine learning, IoT device type identification using machine learning, Keystroke dynamics, Malicious URL detector, Deep-pwning Deep learning-based system for the automatic detection of software vulnerabilitiesAutomatic Intrusion Detection: Spam filtering using machine learning, Phishing URL detection, Capturing network traffic, Network behavior anomaly detection, Botnet traffic detection, Insider threat detection, Detecting DDoS, Credit card fraud detection, Counterfeit bank note detection, Ad blocking using machine learning, Wireless indoor localization

Module 4

Securing and Attacking Data with Machine Learning: Assessing password security using ML, Deep learning for password cracking, Deep steganography, ML-based steganalysis, ML attacks on PUFsEncryption using deep learning, HIPAA data breaches – data exploration and visualization.

Secure and Private AI: Federated learning Encrypted computation, Private deep learning prediction, Testing the adversarial robustness of neural networks, Differential privacy using TensorFlow Privacy

Core Compulsory Readings

1. Machine Learning for Cybersecurity Cookbook- Emmanuel Tsukerman, Packt Publishing

Suggested Readings

1. Hands-On Machine Learning for Cybersecurity - Soma Halder , Sinan Ozdemir, Packt Publishing
2. Machine Learning for Red Team Hackers: Learn The Most Powerful Tools in Cybersecurity -Emmanuel Tsukerman
3. Machine Learning In Cybersecurity A Complete Guide - Gerardus Blokdyk, 5STARCooks publishers

TEACHING LEARNING STRATEGIES

- Hands-on-oriented lecturing, collaborative learning, case studies and project presentations, and peer-led discussions.

MODE OF TRANSACTION

- Lecture, seminar, discussion, audio and video presentation, demonstration, practical assignments, and exercises.

ASSESSMENT RUBRICS

Component	**Marks**
End Semester Evaluation	**60**
Continuous Evaluation	**40**
• Seminar Internal	10
• Case studies / Project(individual)	10
• Assignments	05

• Test	15
Total	**100**

Sample Questions to test Outcomes.

1. How can machine learning be used to detect and prevent malware attacks?
2. What are the key challenges in applying machine learning to cybersecurity?
3. How does anomaly detection using machine learning help in identifying potential security breaches?
4. What types of machine learning algorithms are commonly used for intrusion detection in network security?
5. How can machine learning techniques be employed to classify and identify phishing emails?

SEMESTER II
ELECTIVE COURSE
PDCS02E08CLOUD SECURITY

Course Description

This course provides an in-depth understanding of cloud security principles, practices, and technologies. It covers various aspects of securing cloud-based environments, including infrastructure security, data protection, identity and access management, network security, and compliance.

Course Objectives

- Understand Cloud Computing Basics
- Identify Cloud Security Challenges
- Learn Cloud Security Architecture
- Explore Cloud Provider Security
- Understand Virtualization and Container Security
- Implement Cloud Security Controls
- Explore Cloud Security Best Practices
- Gain Awareness of Emerging Cloud Security Trends

Credit			Teaching Hours			Assessment		
L/T	P/I	Total	L/T	P/I	Total	CE	ESE	Total
4	-	4	2	2	4	40	60	100

Lecture/Tutorials, P/I=Practical/Internship, CE =Continuous Evaluation, ESE = End Semester Evaluation

COURSE OUTCOMES

Course Learning Outcomes: At the end of the Course, the Student will be able to -

C01	Understand the fundamentals of cloud computing
C02	Identify and assess the security challenges and risks associated with cloud computing.
C03	Design and implement secure cloud architectures, considering network security, identity and access management, encryption, and secure data storage
C04	Evaluate and analyse the security measures implemented by cloud service providers.
C05	Understand the legal and compliance requirements related to cloud computing
C06	Stay informed about emerging trends, technologies, and threats in cloud security, and adapts knowledge and skills to address evolving challenges.

*Course outcomes based on revised blooms taxonomy

COURSE CONTENTS

Module 1:

Basics of the Cloud: Cloud Computing- What is cloud computing? why is it used, and what are the benefits, On-premises vs Hosted Solutions, Cloud service models- SaaS, PaaS, IaaS, Types of clouds- Discussion of public, private, hybrid, community, multitenancy, and single tenancy architectures. Augmenting Security with Cloud services- Discussion of Anti-malware, vulnerability scanning, sandboxing, content filtering, cloud security broker, security as a service, and managed security service provider.

Module 2:

Introduction to Cloud Computing and Security: Cloud security challenges and benefits,Cloud Infrastructure Security: Virtualization security, Hypervisor security, Container security, Securing cloud storage. Data Protection in the Cloud: Data encryption techniques, Key management in the cloud, Secure data storage and backup. Identity and Access Management (IAM) in the Cloud:

User provisioning and management, Authentication, and authorization, Single sign-on (SSO) in the cloud

Module 3:

Virtualization: The deployment model-Recap the Azure deployment model with an example. Virtual Machine (VM) Types, Virtual Network Capabilities. Network Security in Cloud Environments: Virtual private networks (VPNs), Firewalls and intrusion detection/prevention systems, Network segmentation and isolation, Cloud Application Security: Secure development lifecycle for cloud applications, Application security testing in the cloud, API security and web application firewalls (WAFs), Cloud Security Auditing and Monitoring: Security event logging and monitoring, Threat detection and incident response in the cloud, Cloud security assessment and auditing

Module 4:

Compliance and Legal Considerations: Cloud security regulations and standards (e.g., GDPR, HIPAA), Cloud-specific compliance frameworks (e.g., CSA STAR, FedRAMP), Cloud Security Tools and Services: Cloud security platforms and solutions, Security automation and orchestration tools, Cloud-native security services, Case Studies, and Best Practices: Analysis of real-world cloud security breaches, best practices for securing cloud environments Data Security Considerations: Discussion of vulnerabilities associated with single server hosting, hosting multiple data types, and a single platform hosting multiple data types/owners on multiple VMs. Security Threats.

Core Compulsory Readings

1. Cloud Computing: Concepts, Technology & Architecture by Thomas Erl, Ricardo Puttini, and Zaigham Mahmood.
2. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance by Tim Mather, Subra Kumaraswamy, and Shahed Latif.
3. Virtualization and Forensics: A Digital Forensic Investigator Guide to Virtual.
4. Environments by Diane Barrett and Greg Kipper.

5. Container Security: Fundamental Technology Concepts that Protect ContainerizedApplications by Liz Rice Winkler.

Suggested Readings

1. Cloud Security: A Comprehensive Guide to Secure Cloud Computing by Ronald L. Krutz and Russell Dean Vines.
2. Data Protection and Privacy in Cloud Services by Stefanos Gritzalis and Javier Lopez.
3. Network Security in Virtualized Data Centers for Dummies by Lawrence C. Miller.
4. Cloud Security and Control: Issues, Challenges, and Best Practices by Victor Chang,Muthu Ramachandran, and Erisa Karafili.
5. Securing Cloud Services: A Pragmatic Approach by Lee Newcombe.
6. Auditing Cloud Computing: A Security and Privacy Guide by Ben Halpert.
7. Cloud Computing and Security: Second International Conference, ICCCS 2016 by Xingming Sun, Dongqing Xie, and Kim-Kwang Raymond Choo.
8. Cloud Computing Security: Foundations and Challenges by John Vacca.
9. Securing the Cloud: Cloud Computer Security Techniques and Tactics by Vic (J.R.).

TEACHING LEARNING STRATEGIES

- Hands-on-oriented lecturing, collaborative learning, case studies and project presentations, and peer-led discussions.

MODE OF TRANSACTION

- Lecture, Seminar, Discussion, audio and video presentation, demonstration, practical assignments and exercises.

ASSESSMENT RUBRICS

Component	Marks
End Semester Evaluation	**60**
Continuous Evaluation	**40**

Sample

• Seminar Internal	10
• Case studies / Project(individual)	10
• Assignments	05
• Test	15
Total	**100**

Questions to test Outcomes.

1. What are the best practices for securing data in the cloud?
2. How does encryption play a role in ensuring data security in the cloud?
3. What are the main authentication and access control mechanisms used in cloud environments?
4. How can you ensure the confidentiality and integrity of data in transit within a cloud environment?
5. What are the security considerations when using multi-tenant cloud services?
6. How can you monitor and detect security breaches or suspicious activities in a cloud environment?