KANNUR UNIVERSITY
കണ്ണൂർ സർവകലാശാല

(Abstract)

FYUG B.Sc. Cyber Security Programme- Scheme and Syllabus of Vth & VI semesters) - Approved & Implemented for 2024 admission - Orders Issued

---

ACADEMIC C SECTION

ACAD C/ACAD C3/8508/2019 Dated: 26.09.2026

Read:-1. U.O. No. FYUGPSC/FYSC-III/9089/2024, dated: 26/03/2025

2. U.O No. ACAD/ACAD C3/8508/2019 dated: 04/07/2025

3. U.O No. ACAD/ACAD C3/8508/2019 dated: 24/12/2025

4. U.O No. ACAD/ACAD C3/8508/2019 dated: 30/04/2026

5. U.O No. ACAD/ACAD C3/8508/2019 dated: 09/06/2026

6.Minutes of the meeting of the Expert Committee held on 06/08/2026

7.Minutes of the online meeting of the Board of studies in Computer science (UG) held on 03/09/2026

8.Email dated, 17.09.2026 of the Dean, Faculty of Technology

9.Orders of Vice Chancellor in the even file dated 18.09.2026

ORDER

1.The Scheme (full) and Syllabus (First & Second Semesters only) of the FYUG B.Sc. Cyber Security Programme was approved and implemented w. e. f 2024 Admission vide the paper read (1) above.

2. As per paper read (2) above, an Expert Committee was constituted for the preparation of syllabi and fixing the eligibility criteria for the FYUG B.Sc. Cyber Security and B.Sc .Data Analytics Programmes.

3.As per paper read (3) above, the scheme (full) and Syllabus (1-4 semesters) of the FYUG B.Sc. Cyber Security Programme (2025 admission) and the modified Scheme (3-8 semesters) and Syllabus (3-4 semesters) of the FYUG B.Sc. Cyber Security Programme (2024 admission) was approved and implemented.

4.Vide paper read (4) above,the Expert Committee was reconstituted for the preparation of syllabi and fixing the eligibility criteria for the FYUG B.Sc. Cyber Security and B.Sc .Data Analytics Programmes.

5.Vide paper read (5) above,the Expert Committee was again reconstituted appointing Prof. Rajkumar K.K., Professor, Department of Information Technology as the Convenor.

6.Vide paper read (6) above, the Expert Committee submitted the Scheme and Syllabus of 5-

8 semesters of the FYUG B.Sc. Cyber Security Programme and recommended that the same be placed before the Board of Studies in Computer Science (UG) for consideration.

7.Vide paper read (7) above, the Board of studies in Computer Science (UG) recommended to approve the Scheme and Syllabi of the V&VI Semesters of the FYUG B.Sc. Cyber Security Programme, only for the academic year 2026-27 .

8.The submitted Scheme and Syllabi were forwarded to the Dean, Faculty of Technology,along with the minutes of the meeting of the Board of studies in Computer Science (UG), for remarks and the Dean vide paper read (8) above recommended approval of the same .

9.The Vice Chancellor after considering the recommendation of the Dean, Faculty of Technology and in exercise of the powers of the Academic Council conferred under Section 11(1) Chapter III of the Kannur University Act, 1996 and all other enabling provisions read together with has approved the Scheme and Syllabus (5-6 semesters) of the FYUG B.Sc. Cyber Security Programme and accorded sanction to implement the same for 2024 admission (only) , subject to reporting to the Academic Council.

10.The approved Scheme and Syllabus are appended with this U.O. and uploaded on the University Website

Orders are issued accordingly.

Sd/-

Bindu K P G

Joint Registrar (Acad)

For REGISTRAR

To: 1. The Controller of Examinations (Through PA)
2. The Principals of Affiliated colleges offering the FYUGP Cyber Security programme
3. The Convenor, Expert Committee
4.The Chairperson, Board of Studies in Computer Science (UG)

Copy To: 1. PA to CE (to circulate the same among the sections concerned under Examination Branch)
2. PS to VC/PA to R
3. JR II /EXC I/ EG I/ AR VII (Exam)
4. DR/AR (Academic)
5. Web Manager (to upload on the website)
6. Computer Programmer
7. SF/DF/FC

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

Forwarded / By Order

SECTION OFFICER

Kannur University

CURRICULUM

SYLLABUS

OF

FOUR YEARS UNDER GRADUATE PROGRAMME (FYUGP)

BSc CYBER SECURITY

Under the Choice Based Credit and Semester System (CBCSS)

W.E.F 2024 Admission onwards

PROGRAMME OUTCOME

PO1: Critical Thinking and Problem-Solving-Apply critical thinking skills to analyse information and develop effective problem-solving strategies for tackling complex challenges.

PO2: Effective Communication and Social Interaction-Proficiently express ideas and engage in collaborative practices, fostering effective interpersonal connections.

PO3: Holistic Understanding-Demonstrate a multidisciplinary approach by integrating knowledge across various domains for a comprehensive understanding of complex issues.

PO4: Citizenship and Leadership-Exhibit a sense of responsibility, actively contribute to the community, and showcase leadership qualities to shape a just and inclusive society.

PO5: Global Perspective-Develop a broad awareness of global issues and an understanding of diverse perspectives, preparing for active participation in a globalized world.

PO6: Ethics, Integrity and Environmental Sustainability-Uphold high ethical standards in academic and professional endeavours, demonstrating integrity and ethical decision-making. Also acquire an understanding of environmental issues and sustainable practices, promoting responsibility towards ecological well-being.

PROGRAMME SPECIFIC OUTCOME

PSO1: Design, apply and implement computer science knowledge to implement robust software solutions using diverse programming languages and design tools.

PSO2: Utilize advanced techniques for data storage, retrieval, and manipulation across varied computing environments

PSO3: Critically evaluate and apply information technology tools and methodologies with ethical consideration

PSO4: Engage in team-based projects and interdisciplinary research to address complex computer science challenges

PSO5: Ability to analyse a problem, and identify and define the security related issues appropriate to its solution.

PSO6: Ability to design, implement, and evaluate a security system and IoT structures that capable of identify, prevent and protect from malware attack.

PSO7: Expose the students to learn the important of Cyber Security such as Web security, intrusion detection and biometric security so that they can have an opportunity to be a part of industry 5.0applications irrespective of domains.

Eligibility for Admission:

Basic qualifications:

Candidate must possess

1) Pass with 50% marks or equivalent grade at 10+2 level or equivalent

AND

2) Mathematics / Statistics / Computer Science / Computer Application / Informatics Practices as one of the subjects at 10+2 level.

Kannur University

BSC CYBER SECURITY
SEMESTER-WISE COURSE STRUCTURE

SEMESTER-1

SI.No.	Course	Course Name	Practical	Credit
1	AEC1	English Department	Yes	3(2T+1P)
2	AEC2	Languages		3
3	MDC1	Multi-Disciplinary Course1		3
4	Major1	Fundamentals of Computers And Computer Security		4
5	Minor1	Optional Minor offered by any department.		4
6	Minor2	Optional Minor offered by any department.		4
Total Credits				**21**

SEMESTER-2

SI.No.	Course	Course Name	Practical	Credit
1	AEC3	English Department	Yes	3(2T+1P)
2	AEC4	Languages		3
3	MDC2	Multi-Disciplinary Course2		3
4	Major2	Operating System	Yes	4(3T+1P)
5	Minor3	Optional Minor offered by any department.		4
6	Minor4	Optional Minor offered by any department.		4
Total Credits				**21**

SEMESTER 3

SI.No.	Course	Course Name	Practical	Credit
1	Major3	Database Management System	Yes	4(3T+1P)
2	Major4	Computer Networks		4
3	VAC1	Value Added Course 1		3
4	Minor5	Optional Minor offered by any department.		4
5	Minor6	Optional Minor offered by any department.		4
6	MDC3	Multi-Disciplinary Course3(KS) Offered by English and language department		3
Total Credits				**22**

SEMESTER 4

SI.No.	Course	Course Name	Practical	Credit
1	Major5	Web Technology and Web Security	Yes	4(3T+1P)
2	Major6	Python Programming	Yes	4(3T+1P)
3	Major 7	Information Security		4
4	SEC1	Skill Enhancement Course 1	Yes	3(2T+1P)
5	VAC2	Value Added course 2		3
6	VAC3	Value Added course 3		3
Total Credits				**21**

SEMESTER 5

SI.No.	Course	Course Name	Practical	Credit
1	Major8	Ethical Hacking	Yes	4(3T+1P)
2	Major9	System and Network Security	Yes	4(3T+1P)
3	Major 10	Malware Forensics		4
4	Major11	Discipline Specific Elective		4
5	Major12	Discipline Specific Elective		4
6	SEC2	Skill Enhancement Course 2		3
7	Internship			**2**
Total Credits				**25**

SEMESTER -6

SI.No.	Course	Offering Departments	Practical	Credit
1	Major13	Vulnerability Assessment and Penetration Testing	Yes	4(3T+1P)
2	Major14	Cyber Forensic		4
3	Major 15	Cloud Security		4
4	Major16	Discipline Specific Elective		4
5	Major17	Discipline Specific Elective		4
6	SEC3	Skill Enhancement Course 3		3
Total Credits				**23**

LIST OF COURSES

Semester: 1

Course Code	Title of the Course	Type of the Course DSC, MDC, SEC etc.	Credit	Hours / week	Hour Distribution /Week			
					L	T	P	O
KU1DSCCSY101	Fundamentals of Programming with C	DSC	4 (3T+1P)	5	3		2	
KU1DSCCSY102	Fundamentals of Computers And Computer Security	DSC	4	4	4		0	
KU1DSCCSY103	Major Trends in Information Technology	DSC	4	4	4		0	
KU1MDCCSY101	Introduction to Cyber Security	MDC	3	3	3		0	

L — Lecture, T — Tutorial, P — Practical/Practicum

AEC- Ability Enhancement Course, DSC- Discipline Specific Course, SEC- Skill Enhancement Course, VAC- Value Added Course, DSE- Discipline Specific Elective

Semester: 2

Course Code	Title of the Course	Type of the Course DSC, MDC, SEC etc.	Credit	Hours / week	Hour Distribution /Week			
					L	T	P	O
KU2DSCCSY104	Operating System	DSC	4 (3T+1P)	5	3		2	
KU2DSCCSY105	Object Oriented Programming using C++	DSC	4 (3T+1P)	5	3		2	
KU2MDCCSY102	Digital Empowerment Through Ethical Standards	MDC	3	3	3			

Semester: 3

Course Code	Title of the Course	Type of the Course DSC, MDC, SEC etc.	Credit	Hours / week	Hour Distribution /Week			
					L	T	P	O
KU3DSCCSY201	Data Base Management System	DSC	4 (3T+1P)	5	3		2	
KU3DSCCSY202	Computer Networks	DSC	4	4	4			
KU3DSCCSY203	Programming in Java	DSC	4 (3T+1P)	5	3		2	
KU3VACCSY201	Cyber Laws and Rules	VAC	3	3	3			

Semester: 4

Course Code	Title of the Course	Type of the Course DSC, MDC, SEC etc.	Credit	Hours / week	Hour Distribution /Week			
					L	T	P	O
KU4DSCCSY204	Web Technology And Web Security	DSC	4 (3T+1P)	5	3		2	
KU4DSCCSY205	Fundamentals of Cyber Security	DSC	4 (3T+1P)	5	3		2	
KU4DSCCSY206	Python Programming	DSC	4 (3T+1P)	5	3		2	
KU4DSCCSY207	Information Security	DSC	4	4	4		0	
KU4SECCSY201	Linux System And Network Administration	SEC	3 (2T+1P)	4	2		2	
KU4VACCSY202	Cyber Ethics	VAC	3	3	3			
KU4VACCSY203	FOSS for Cyber Security	VAC	3	3	3			

Semester: 5

Course Code	Title of the Course	Type of the Course DSC, MDC, SEC etc.	Credit	Hours / week	Hour Distribution /Week			
					L	T	P	O
KU5DSCCSY301	Ethical Hacking	DSC	4 (3T+1P)	5	3		2	
KU5DSCCSY302	System and Network Security	DSC	4 (3T+1P)	5	3		2	
KU5DSCCSY303	Malware Forensics	DSC	4	4	4			
KU5DSECSY301	Database Security	DSE	4 (3T+1P)	5	4			
KU5DSECSY302	Blockchain Technology	DSE	4	4	4			
KU5DSECSY303	MOOC / Online Course	DSE	4					
KU5SECCSY301	Biometric security	SEC	3	3	3			
KU5INTERN301	INTERNSHIP	DSC	2					

Semester: 6

Course Code	Title of the Course	Type of the Course DSC, MDC, SEC etc.	Credit	Hours / week	Hour Distribution /Week			
					L	T	P	O
KU6DSCCSY304	Vulnerability Assessment and Penetration Testing	DSC	4 (3T+1P)	5	3		2	
KU6DSCCSY305	Cyber Forensic	DSC	4	4	4			
KU6DSCCSY306	Cloud Security	DSC	4	4	4			
KU6DSECSY304	AI Driven Software Engineering	DSE	4 (3T+1P)	5	3		2	
KU6DSECSY305	AI For Cyber Security	DSE	4 (3T+1P)	5	3		2	
KU6DSECSY306	MOOC / Online Course	DSE	4					
KU6SECCSY302	IoT Security	SEC	3	3	3			

DETAILED SYLLABUS

KU1DSCCSY101: FUNDAMENTALS OF PROGRAMMING WITH C

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
1	DSC	100-199	**KU1DSCCSY101**	4 (3T+1P)	75

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
3	2		35	65	100	1.5hrs.

Course Description:

This course introduces the fundamental concepts of programming using C language. Student will learn about data types, control structures, functions, arrays, pointers, and file handling. Emphasis is placed on developing logical thinking and problem solving skills through hands-on programming exercises. By the end of course, students will be able to design, implement, and debug basic C programs.

Course Prerequisite: NIL

Course Outcomes:

CO No.	Expected Outcome	Learning Domains
1	Identify the basic syntax and structure of the C programming language.	U, A
2	Design algorithms and flowcharts to represent simple problems.	U, A
3	Understand and use various program control structures.	U, A
4	Implement arrays and strings using appropriate logic	U, A, E

****Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)***

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	3			2			
CO 2	3		2				
CO 3	3	3	3	2			
CO 4	3	2	2	2		2	2

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	UNIT	DESCRIPTION	HOURS
1	**MODULE 1: Introduction to Programming**		
	1	Programming languages, compilers, compiling and executing a program. Representation of Algorithm - Algorithms for finding roots of quadratic equations, finding minimum and maximum numbers of a given set, finding if a number is prime number. Flowchart and Pseudocode with examples, Program design and structured programming.	15
	2	Introduction to C Programming Language: Character set, constants, variables (with data types and space requirements), printf(), scanf()	
	3	Syntax and Logical Errors in compilation, object and executable code, Operators, expressions and precedence, Expression evaluation, Storage classes (auto, extern, static and register), type conversion. The main function and command line arguments. Bitwise operations: Bitwise AND, OR, XOR and NOT operators.	
	4	Conditional Branching and Loops: Writing and evaluation of conditionals and consequent branching with if, if-else, switch-case, ternary operator, goto, Iteration with for, while, do- while loops.	
2	**MODULE 2: Functions and Dynamic Memory Allocation**		
	1	Functions: Designing structured programs, declaring a function,	15

		structure of a function, Parameters and return type of a function.	
	2	Passing parameters to functions, call by value, passing arrays to functions, passing pointers to functions, idea of call by reference,	
	3	Library functions in C, Recursion: Simple programs, such as Finding Factorial, Fibonacci series etc., Limitations of Recursive functions.	
	4	Dynamic memory allocation: Allocating and freeing memory, Allocating memory for arrays of different data types.	

3	**MODULE 3: Arrays, Structures and Pointers**		
	1	Arrays: one and two-dimensional arrays, creating, accessing and manipulating elements of arrays.	15
	2	Strings: Introduction to strings, handling strings as array of characters, basic string functions available in C (strlen, strcat, strcpy, strstr etc.), arrays of strings.	
	3	Structures: Defining structures, initializing structures, unions, Array of structures.	
	4	Pointers: Idea of pointers, Defining pointers, Pointers to Arrays and Structures, Use of Pointers in self-referential structures, usage of self referential structures in linked list (no implementation) ,Enumeration.	

4	**MODULE 4: Preprocessor and File handling in C**		
	1	Preprocessor: Commonly used Preprocessor commands like include, define, undef, if, ifdef, ifndef.	
	2	Files: Text and Binary files, Creating and Reading and writing text and binary files,	
	3	Appending data to existing files, Writing and reading structures using binary files.	
	4	Random access using fseek, ftell and rewind functions.	

5	**Teacher Specific Module**		
	Directions		
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends,		15

	thereby enabling students to gain both theoretical knowledge and contextual understanding.	

Essential Readings

1. Balagurusamy, E. *Programming in ANSI C*. Tata McGraw-Hill, 1994.
2. Kanetkar, Yashavant P. *Let Us C*. 16th ed., BPB Publications, 2017.

Suggested Readings

1. Kernighan, Brian W., and Dennis M. Ritchie. *The C Programming Language*. 2nd ed., Prentice Hall, 1988.
2. Gottfried, Byron S. *Schaum's Outline of Programming with C*. 2nd ed., McGraw-Hill, 1996.

Assessment Rubrics:

Evaluation Type		**Marks**
End Semester Evaluation		**50 (Theory)** **15 (Practical)**
Continuous Evaluation		**35**
CE (Theory)		**25**
a)	Test Paper- 1	5
b)	Model Exam	10
c)	Assignment(2 numbers)	5
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
CE (Practical)		**10**
Total		**100**

KU1DSCCSY102: FUNDAMENTALS OF COMPUTERS AND COMPUTER SECURITY

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
1	DSC	100-199	**KU1DSCCSY102**	4	75

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
4	0		30	70	100	2hrs.

Course Description:

This course describes the basic principles, components, and operations of computer systems, covering essential knowledge for using computers effectively, understanding hardware and software, and grasping concepts like data representation, operating systems, and Computer Security.

Course Prerequisite: NIL

Course Outcomes:

CO No.	Expected Outcome	Learning Domains
1	Identify various components of computer system and understand their functions.	U
2	Demonstrate data representation in computer system and various.	U
3	Compare the performance of different types of software.	An
4	Understand the fundamental concepts of Computer Security.	U

**Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)*

Mapping of Course Outcomes to PSOs

	PSO	PSO	PSO	PSO	PSO	PSO	PSO

	1	2	3	4	5	6	7
CO1	3	2					
CO2	3						
CO3	2		2				
CO4	3		3				2

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	UNIT	DESCRIPTION	HOURS
	MODULE 1: Introduction to Computers		
1	1	Definition and Characteristics of Computers, Brief History and Evolution of Computers. Computer System Overview, Basic Components of a Computer System - Input, Output, Processing, and Storage.	15
	2	**Central Processing Unit (CPU):** Basic Concepts of CPU, Function and Components, Architecture of a CPU - ALU, Registers, and Control Unit.	
	3	Computer Memory: Memory Hierarchy - An Overview, Primary Memory - RAM (Random Access Memory) and ROM (Read-Only Memory), Secondary Memory.	

	MODULE 2: Introduction to Data Representation		
2	1	Decimal, Binary, Hexa-Decimal and Octal Number Systems, Conversion Between Number Systems.	15
	2	Binary Arithmetic and Complements: Binary addition, subtraction, Complements of Binary Numbers (1's Complement and 2's	

		Complement).	
	3	Binary Coding Scheme: EBCDIC, ASCII Code, Unicode.	
	4	Logic Gates: AND, OR, NOT, NAND, NOR, XOR, XNOR.	

3	**MODULE 3: Introduction to Software**		
	1	Types of Software - Application Software, System Software.	15
	2	Operating Systems – introduction, Objectives of Operating System, Types of Operating System, Examples.	
	3	Linux Operating System: Features of Linux. Basic Commands – useradd, passwd, ls, mkdir, rmdir, cd, cp, mv, rm, pwd,cat.	

	MODULE 4: Introduction to Computer Security		
4	1	Introduction, Security Threat and Security attack, Malicious Software: Virus- Worms –Trojan Horse.	15
	2	Hacking: Packet Sniffing-Password Cracking – E-mail Hacking, Security Services.	
	3	Users Identification and Authentication: User Name and Password- Smart card- Biometric Techniques. Security Policy.	

5	**Teacher Specific Module**	**15**
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	

Essential Readings:

1. Goel, Anita. *Computer Fundamentals*. Pearson Education India, 2010.

2. Floyd, Thomas L. *Digital Fundamentals*. 10th ed., Pearson Education India (UBS), 2011.

3. Petzold, Charles. *Code: The Hidden Language of Computer Hardware and Software*. Pearson Education, 2022

4. Kanetkar, Yashavant P. *Unix Shell Programming*. BPB Publications, 1996.

Assessment Rubrics:

Evaluation Type		**Marks**
End Semester Evaluation		**70**
Continuous Evaluation		**30**
a)	Test Paper- 1	5
b)	Model Exam	10
c)	Assignment(2 numbers)	10
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
Grand Total		**100**

KU1DSCCSY103: MAJOR TRENDS IN INFORMATION TECHNOLOGY

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
1	DSC	100-199	**KU1DSCCSY103**	4	75

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
4	0		30	70	100	2hrs.

Course Description:

This course explores the latest trends and innovations in information technology. Students will learn about emerging technologies, their impact on the industry, and how to leverage these technologies in real-world applications. Topics include artificial intelligence, blockchain, cloud computing, cybersecurity, the Internet of Things (IoT), big data analytics, and more.

Course Prerequisite: NIL

Course Outcomes:

CO No.	Expected Outcome	Learning Domains
1	Identify the impact of emerging technologies in the field of IT and real life	U
2	Judge the impact of these technologies on various industries.	An
3	Examine practical applications and case studies of emerging technologies.	A
4	Critically evaluate problem-solving skills in the context of new technological developments.	A/E

**Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)*

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	1	2	2	3			
CO 2	1	2	2	3			
CO 3	1	2	2	3			
CO 4	1	2	2	3			

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	UNIT	DESCRIPTION	HOURS
1	**MODULE TITLE:** Introduction to Emerging Technologies		15
	1	Overview of current trends in IT The importance of staying updated with technology	
	2	Edge Computing and 5G Technology-Fundamentals of edge computing.	
	3	The impact of 5G on IT infrastructure Examples of edge computing applications	

2	**MODULE TITLE: A**rtificial Intelligence and Machine Learning*		15
	1	Fundamentals of AI and ML	
	2	Applications in various industries	
	3	Ethical considerations and challenges	

3	**MODULE TITLE :** Internet of Things (IoT) &Cloud Computing		15
	1	Overview of IoT and its components	

		Applications in smart homes, healthcare, and industrial automation	
	2	Security and privacy concerns	
	3	Cloud Computing- Introduction and Architecture	
	4	Types of cloud services (IaaS, PaaS, SaaS)	
	5	Benefits and challenges of cloud adoption	

4	**MODULE TITLE: Cybersecurity Trends and Ethical and Social Implications of Emerging Technologies***		**15**
	1	Current cyber security threats and vulnerabilities	
	2	Emerging security technologies and practices- The role of AI in cybersecurity	
	3	Ethical considerations in the development and deployment of new technologies - Social impact and the digital divide	
	4	Regulatory and policy issues	

5	**Teacher Specific Module**	
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	15

Essential Readings:

1. Russell, Stuart J., and Peter Norvig. *Artificial Intelligence: A Modern Approach*. 4th ed., Pearson, 2020.
2. Erl, Thomas, with Ricardo Puttini and Zaigham Mahmood. *Cloud Computing: Concepts, Technology & Architecture*. Prentice Hall, 2013.
3. Singer, P. W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford University Press, 2014.

Assessment Rubrics:

Evaluation Type		Marks
End Semester Evaluation		**70**
Continuous Evaluation		**30**
a)	Test Paper- 1	5
b)	Model Exam	10
c)	Assignment(2 numbers)	10
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
Grand Total		**100**

KU1MDCCSY101: INTRODUCTION TO CYBER SECURITY

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
1	MDC	100-199	**KU1MDCCSY101**	3	45

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
3	0	-	25	50	75	1.5 hrs

Course Description:

This course provides an overview of the principles and practices of cyber security. Students will learn about the fundamental concepts of Networks, common threats and vulnerabilities, and strategies for protecting systems and data.

Course Prerequisite: NIL

Course Outcomes:

CO No.	Expected Outcome	Learning Domains
1	Understand the fundamental concepts of Cyber Security.	U
2	Understand the fundamental concepts of Computer Networks.	U
3	Identify various types of cyber threats and vulnerabilities.	An
4	Implement security measures and best practices.	C

****Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)***

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	3	3	2	2			
CO 2	2	3	2	2			

CO 3	3	3	2	3			
CO 4	2	3	2	3			

COURSE CONTENTS

MODULE	UNIT	DESCRIPTION	HOURS
1	**MODULE TITLE: Introduction to Cyber Security**		
	1	Introduction, Need for Cyber Security, Data and Information.	9
	2	Cyber Security terminology - Cyberspace, Cybercrime, Cyber-attack, Threat, Vulnerability, Malware, Phishing, Botnets, Adware, Denial of Service , Ransomware, Key Logger.	
	3	The CIA Triads- Confidentiality, Integrity and Availability. Consequences of Weak Security, Challenges in Cyber Security.	
2	**MODULE TITLE: Introduction to Computer Security**		
	1	Introduction, Security Threat and Security attack, Malicious Software: Virus- Worms –Trojan Horse.	9
	2	Hacking: Packet Sniffing-Password Cracking – E-mail Hacking, Security Services.	
	3	Users Identification and Authentication: User Name and Password- Smart card- Biometric Techniques. Security Policy.	
3	**MODULE TITLE: Network Fundamentals**		
	1	Understanding networks - LAN, WAN, VPN, MAN, PAN	9
	2	OSI Model, OSI Layer Security, TCP/IP model.	
	3	IP address: Types of IP addresses (private IP address, Public IP address), IP address classification. WWW, Internet.	

	MODULE TITLE: Network Security Fundamentals		
4	1	Need for Network Security, Hacking, stages of Hacking, Ethical hacking.	9
	2	Types of Network attacks- Spoofing, Sniffing, Mapping, Hijacking, Trojans, DoS and DDoS.	
	3	Firewalls- Types of firewalls, intrusion detection/prevention systems (IDS/IPS).	

5	**Teacher Specific Module**	**9**
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	

Essential Readings:

1. Agrawal, Narmrata. *Cyber Security: A Complete Solution*. Dreamtech Press, 2018.
2. Goutam, Rajesh Kumar. *Cybersecurity Fundamentals*. BPB Publications, 2021.
3. Graham, James, Ryan Olson, and Rick Howard, editors. *Cyber Security Essentials*. Auerbach Publications, 2010.

Assessment Rubrics:

Evaluation Type	Marks
End Semester Evaluation	**50**
Continuous Evaluation	**25**

a)	Test Paper- 1	5
b)	Model exam	10
c)	Assignment	5
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
Total		**75**

KU2DSCCSY104: OPERATING SYSTEM

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
2	DSC	100-199	**KU2DSCCSY104**	4 (3T+1P)	75

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
3	2	-	35	65	100	1.5hrs.

Course Description:

This course provides a comprehensive introduction to the fundamental concepts and principles of operating systems. It covers the core components, including process management, memory management, file systems, and I/O systems. The course also includes a practical, hands-on module focused on the Linux operating system, giving students the skills to manage and interact with a real-world OS.

Course Prerequisite: Basic understanding of computer

Course Outcomes:

CO No.	Expected Outcome	Learning Domains
1	Students will understand the fundamental functions and types of operating systems.	U
2	They will be able to explain different process management and CPU scheduling techniques.	U, A
3	Students will understand the principles of memory management and virtual memory.	U

4	They will gain practical skills in using basic Linux commands and managing the Linux file system.	A

**Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)*

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	3						
CO 2	3						
CO 3	3						
CO 4			3				

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	UNIT	DESCRIPTION	HOURS
1	**MODULE 1: Introduction to Operating System**		
	1	Definition and structure of OS, Functions of OS. Types of Operating Systems. Batch OS, Multi programming OS, Time Sharing OS, Real time OS, Distributed OS. User mode and Kernel mode, System Calls (Introduction only)	15
	2	Process management: process concept, process state, process control block, process scheduling, operations on processes, cooperating processes.	
	3	CPU scheduling, scheduling criteria, CPU scheduling algorithms.	
	4	Deadlocks Characterization, Resource Allocation Graph, Dead lock prevention and avoidance.	
2	**MODULE 2: Memory Management in Operating System**		

	1	Memory management, contiguous memory allocation,	10
	2	Paging, segmentation, segmentation with paging.	
	3	Virtual memory, demand paging, page replacement	

3	**MODULE 3: File System**		
	1	Access Methods: Sequential, Direct, Other access methods. Allocation Methods: Contiguous allocation, Linked Allocation, Indexed Allocation	15
	2	Directory Structure: Single- level Directory, Two- level Directory, Tree -structured directories.	
	3	I/O systems-Kernel I/O subsystem-I/O Scheduling, Buffering, caching, Spooling.	

4	**MODULE 4: Linux Operating System**		
	1	Architecture, Features of Linux OS, Types of Users, add user and delete user.	20
	2	Linux File system, Types of files in Linux, security by file permissions.	
	3	Linux commands: pwd, cp, rm, mv, cat, cd, absolute and relative paths, ls, mkdir, rmdir, chmod. vi editor. Monitoring Processes: Using top, htop, and ps with various flags (-ef, aux)	
	4	Mounting, Linux Installation.	

5	**Teacher Specific Module**	
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and	15

	contextual understanding.	

Essential Readings:

1. Silberschatz, Abraham, Peter B. Galvin, and Greg Gagne. *Operating System Concepts*. Wiley, 2018.
2. Frisch, Æleen. *Essential System Administration*. O'Reilly & Associates, 2002.
3. Kerrisk, Michael. *The Linux Programming Interface: A Linux and UNIX System Programming Handbook*. No Starch Press, 2010.

Suggested Readings:

1. Tanenbaum, Andrew S., and Herbert Bos. *Modern Operating Systems*. Pearson, 2015.
2. Gilly, Daniel. *Unix in a Nutshell*. O'Reilly & Associates, 1992.
3. Nemeth, Evi, et al. *Linux Administration Handbook*. Prentice Hall, 2006.
4. Negus, Christopher. *Red Hat Linux Bible*. Wiley, 2010.
5. Thomas, Rebecca, and Jean Yates. *A User Guide to the UNIX System*. Tata McGraw-Hill, 1984.

Assessment Rubrics:

Evaluation Type		**Marks**
End Semester Evaluation		**50 (Theory)** **15 (Practical)**
Continuous Evaluation		**35**
CE (Theory)		**25**
a)	Test Paper- 1	5
b)	Model Exam	10
c)	Assignment(2 numbers)	5
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
CE (Practical)		**10**
Total		**100**

\

KU2DSCCSY105: OBJECT ORIENTED PROGRAMMING USING C++

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
2	DSC	100-199	**KU2DSCCSY105**	4 (3T+1P)	75

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
3	2	-	35	65	100	1.5hrs.

Course Description:

This course introduces the fundamentals of C++ programming with a focus on Object-Oriented Programming (OOP) principles such as encapsulation, inheritance, polymorphism, and abstraction. Students will develop skills to design and implement object-oriented applications.

Course Prerequisite: NIL

Course Outcomes:

CO No.	Expected Outcome	Learning Domains
1	Understand the core principles of object-oriented programming.	U, A
2	Learn the syntax and semantics of the C++ programming language	U, A
3	Apply OOP principles to solve real-world programming problems	U, A
4	Develop small to medium-scale C++ applications using classes and objects	U, A, E

**Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)*

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	3			2			
CO 2	3		2				
CO 3	3	3	3	2			
CO 4	3	2	2	2		2	2

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	UNIT	DESCRIPTION	HOURS
1	**MODULE 1: Introduction to OOP and C++ Basics**		
	1	Procedural vs Object-Oriented Programming	15
	2	OOP Concepts: Encapsulation, Inheritance, Polymorphism, Abstraction	
	3	Structure of a C++ Program	
	4	Data Types, Operators, and Basic Input/Output	

2	**MODULE 2: Input/Output and Branching**		
	1	Control Structures: Branching and Looping	15
	2	Defining Classes and Creating Objects	
	3	Member Functions, Constructors, Destructors	
	4	Introduction to Operator Overloading (Unary and Binary – concepts only)	

3	**MODULE 3: Inheritance and Polymorphism**	

	1	Friend Functions and Friend Classes	15
	2	Control statements: break, continue	
	3	Types of Inheritance: Single, Multiple, Multilevel, Hierarchical, and Hybrid (with programs)	

4	**MODULE 4: Virtual Functions and Polymorphism**		
	1	Compile-Time Polymorphism: Function Overloading, Operator Overloading (with examples)	
	2	Runtime Polymorphism: Virtual Functions, Pure Virtual Functions, Abstract Classes and Interfaces.	

5	**Teacher Specific Module**	
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	15

Essential Readings:

1. Balagurusamy, E. *Object-Oriented Programming with C++*. McGraw Hill, 2013.

Suggested Readings:

1. Lafore, Robert. *Object-Oriented Programming in C++*. 4th ed., Sams Publishing, 2002.
2. Stroustrup, Bjarne. *The C++ Programming Language*. 4th ed., Addison-Wesley, 2013.
3. Schildt, Herbert. *C++: The Complete Reference*. 4th ed., McGraw Hill, 2003.
4. Kanetkar, Yashavant P. *Let Us C++*. BPB Publications, 2010.

Assessment Rubrics:

Evaluation Type		**Marks**
End Semester Evaluation		**50 (Theory)** **15 (Practical)**
Continuous Evaluation		**35**
CE (Theory)		**25**
a)	Test Paper- 1	5
b)	Model Exam	10
c)	Assignment(2 numbers)	5
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
CE (Practical)		**10**
Total		**100**

KU2MDCCSY102: DIGITAL EMPOWERMENT THROUGH ETHICAL STANDARDS

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
2	MDC	100-199	**KU2MDCCSY102**	3	45

Learning Approach(Hours/Week)			Marks Distribution			Duration of ESE(Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
3	0	-	25	50	75	1.5hrs.

Course Description: This course explores the evolution from pre-digital challenges to the current digital landscape, covering historical milestones, key technologies, and the vision of Digital India. It emphasizes the benefits and importance of digital revolution while addressing ethical and security considerations. Participants engage with digital tools for personal and professional growth and examine case studies on digital infrastructure, missions, and services to understand real-world applications

Course Prerequisite: NIL

Course Outcomes:

CO No.	**Expected Outcome**	**Learning Domains**
CO1	Understand the evolution of digital technologies and their transformative impact on society, economy, and governance.	U
CO2	Analyze the key initiatives of Digital India and the role of Kerala in becoming a digitally empowered society.	An
CO3	Apply various digital tools for effective communication, collaboration, content creation, and professional development.	A
CO4	Evaluate digital security challenges, privacy issues, and ethical considerations in the use of digital technologies.	E

Remember (R), Understand (U), Apply (A), Analyze (An), Evaluate (E), Create (C)

Mapping of Course Outcomes to PSOs

	PSO1	**PSO2**	**PSO3**	**PSO4**	**PSO5**
CO1	**3**	**2**			

CO2	**3**	**2**			
CO3	**3**	**2**			
CO4	**3**	**2**			

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	UNIT	DESCRIPTION	HOURS
1	**MODULE TITLE: Transition to Digital World**		
	1	Challenges of Pre-Digital Age	**9**
	2	Importance and Benefits of Digital Revolution	
	3	Key concepts: digitization, digitalization, digital transformation	
	4	Introduction to Key Digital Technologies: Cloud Computing, IoT, AI, Block Chain	
2	**MODULE TITLE: Perspective of Digital India & Digital Innovations in Kerala**		
	1	Understanding Digital India: Concept, Objectives, and Evolution	**9**
	2	Overview of Digital Infrastructure: Broadband Connectivity, Digital Literacy, and Access to Information	
	3	Vision of Digital India: DigiLocker, E-Hospitals, ePathshala, BHIM, e-Health Campaigns	
	4	Kerala-Emergence as Digital Society: Internet & Mobile Penetration in Kerala, 4 Pillars of Digital Emergence in Kerala (Akshaya Project, IT@School Project, Digital Infrastructure Availability, State Data Centre & allied Applications)	
	5	Role of K-DISC in Digital Empowerment	
	6	Kerala State IT Mission: Core IT Infrastructure, eGovernance Applications, Service Delivery Platforms	
3	**MODULE TITLE: Digital Tools for Personal and Professional Growth**		
	1	Digital Tools for Data Sharing: Google Drive, Google Sheets	**9**

	2	Digital Tools for Data Sharing: Google Docs, Google Classroom	
	3	Online learning platforms and resources (e.g., Coursera, Khan Academy, MOOCs, Duolingo)	
	4	Networking Tools: LinkedIn	
	5	Content Creation and Management: Canva	
4	**MODULE TITLE: Ethical and Security Considerations in the Digital Age**		
	1	Understanding privacy in the digital age	**9**
	2	Legal and ethical considerations in data collection and processing: Intellectual Property Rights (IPR)	
	3	Key Terminologies: Cyber Security, Cyber Crime, Cyber Attack, Cyber Espionage, Cyber Warfare	
	4	Authentication, Authorisation	
	5	Cyber Crimes and Classification	
	6	Introduction to Cyber Laws in India	
5	**Teacher Specific Module**		**9**
	Directions		
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.		

Essential Readings:

1. S K Kaushal, “Digital India Importance Needs and Values”, N B Publications, 2018.
2. Vipin M. Chaturvedi and Shivani Kapoor, “Cyber Security in India: Government, Law Enforcement and Corporate Sector"
3. R.S. Pressman, G. Sharma, and G. Sridhar, "Information Security: Principles and Practices in Indian Context"
4. Michael Goodrich and Roberto Tamassia, “Introduction to Computer Security”, First Edition, Pearson Education, 2011.

Assessment Rubrics:

Evaluation Type		Marks
End Semester Evaluation		**50**
Continuous Evaluation		**25**
a)	Test Paper- 1	5
b)	Model exam	10
c)	Assignment	5
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
Total		**75**

KU3DSCCSY201: DATABASE MANAGEMENT SYSTEM

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
3	DSC	200-299	**KU3DSCCSY201**	4(3T+1P)	75

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
3	2		35	65	100	1.5 hr

Course Description: This course introduces the basics of Database Management Systems (DBMS).It covers data models, ER diagrams, and database design concepts. Students will learn about keys, relational algebra, and normalization. The course includes hands-on practice with SQL queries and commands. Advanced topics like joins, views, triggers, and functions are also included. By the end, students will be able to design and manage relational databases.

Course Prerequisite: NIL

Course Outcomes:

CO No.	Expected Outcome	Learning Domains
1	Demonstrate a foundational understanding of database systems, data models, and the principles of designing Entity-Relationship (ER) diagrams.	U,A
2	Apply relational algebra operations and normalization techniques to design efficient databases.	U,A
3	Write and execute SQL queries using DDL, DML, and DCL commands for effective data manipulation and control.	U,A,E
4	Use SQL operators, functions, joins, views, triggers, and subqueries for advanced database operations.	U,A,E,C

****Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)***

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	3			2			
CO 2	3		2				
CO 3	3	3	3	2			
CO 4	3	2	2	2		2	2

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	**UNIT**	**DESCRIPTION**	**HOURS**
1	**MODULE 1: Introduction to Database Management System**		
	1	Introduction- Database System Applications, purpose of database system,	15
	2	View of Data- Data Abstraction, Schemas and Instances, Data Models.	
	3	Database Users and Administrators, Transaction Management-ACID Properties.	
	4	ER Model, Basic concepts, ER Diagram, Specialization and generalization.	

2	**MODULE 2: Relational algebra and Normalization**		
	1	Keys: Candidate key, Super key, Primary key, Foreign Key. Functional Dependency -Basic definitions, Trivial and non-trivial dependencies.	15
	2	Normalization- Introduction, Normal forms- 1NF,2NF,3NF, BCNF	
	3	Relational algebra operations.	

3	**MODULE 3: Structured Query Language**		
	1	Introduction to SQL, Datatypes in SQL, Database languages, Integrity Constraints.	15
	2	DDL Commands- create, alter, and drop.	
	3	DML commands – Insert into, select, delete, update.	
	4	DCL Commands – Grant, Revoke.	

4	**MODULE 4: SQL Operators and Functions**		
	1	SQL Operators – Arithmetic, Relational, Logical, Like Operator	15
	2	Aggregate functions- Sum(),avg(),min(),max(),count()	
	3	Character functions, Order by clause, group by clause, having clause, sub query	
	4	View and Sequence, Join Operations- inner and outer join, Triggers, functions	

5	**Teacher Specific Module**	
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	15

Essential Readings:

1. Silbersehatz, Korth and Sudarshan, Database system concepts, 6th edition MGH 2011
2. Ramakrishnan and Gehrke, Database Management Systems, 3rd Edn, McGraw Hill, 2003
3. A Leon & M Leon, Database Management Systems , Leon Vikas – 2003.
4. Elmasri and Navathe, Fundementals of Database systems, 5thEdition ,Pearson 2009
5. O'Reilly, Practical PostgreSQL Shroff Publishers(SPD) 2002
6. C J Date, An Introduction to Database systems, Pearson, 2004.

Assessment Rubrics:

Evaluation Type		Marks
End Semester Evaluation		**50 (Theory)** **15 (Practical)**
Continuous Evaluation		**35**
CE (Theory)		**25**
a)	Test Paper- 1	5
b)	Model Exam	10
c)	Assignment(2 numbers)	5
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
CE (Practical)		**10**
Total		**100**

KU3DSCCSY202: COMPUTER NETWORKS

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
3	DSC	200-299	**KU3DSCCSY202**	4	60

Learning Approach(Hours/Week)			Marks Distribution			Duration of ESE(Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
4	0	-	30	70	100	2Hrs

Course Description:

This course introduces the fundamentals of computer networks, covering network types, topologies, protocols, IP addressing, routing, data communication, and emerging technologies like IoT and cloud networking. Students will gain foundational knowledge of how networks function, communicate, and evolve, preparing them for further studies or careers in networking and IT.

Course prerequisite:NIL

CourseOutcomes :

CO No.	Expected Outcome	Learning Domains
1	Describe the fundamental concepts and architecture of computer networks.	U
2	Explain various networking models, protocols, and transmission techniques.	U
3	Apply addressing schemes and routing algorithms in network communication.	U,A

4	Identify and implement basic network mechanisms and practices.	U,A

**Remember(R), Understand (U), Apply (A), Analyse (An), Evaluate (E),Create(C)*

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	3			2			
CO 2							
CO 3	3		2				
CO 4	3		2				3

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	UNIT	DESCRIPTION	HOURS
1	**MODULE 1: Fundamentals of Computer Networks**		
	1	Introduction to Computer Networks – Uses, Applications, Types (LAN, WAN, MAN, PAN)	12
	2	Network Topologies – Star, Bus, Ring, Mesh; Advantages and Limitations	
	3	Reference Models – OSI and TCP/IP; Comparison and Layer Functions	
	4	Transmission Media – Twisted Pair, Coaxial, Fiber Optic, Wireless Media,	
	5	Switching Techniques – Circuit, Packet, and Message Switching	
2	**MODULE 2: Network Protocols and Data Communication**		
	1	Data Communication Concepts – Signals, Transmission Modes, Bandwidth	12

	2	Error Detection and Correction – Parity Check, CRC, Hamming Code	
	3	Flow Control and Access Control – Stop-and-Wait, Sliding Window, CSMA/CD, CSMA/CA	
	4	IEEE 802 Standards – Ethernet (802.3), Wi-Fi (802.11) ,	
	5	Protocols and Layer-wise Examples (IP, TCP, UDP, HTTP, FTP, DNS)	

3	**MODULE 3: Addressing In Networks**		**12**
	1	IP Addressing – IPv4 Address Classes, Subnetting, Super netting	
	2	Routing Concepts – Static vs. Dynamic Routing, Table-driven Routing	
	3	Routing Algorithms – Distance Vector, Link State	
	4	ICMP, ARP, DHCP, and NAT	
	5	Introduction to IPv6 – Structure, Benefits, Transition from IPv4.	

4	**MODULE 4: Advanced Concepts of Computer Networks**		
	1	Client-Server and Peer-to-Peer Models – Concepts, Applications	12
	2	Network Devices – Repeaters, Hubs, Switches, Routers, Gateways	
	3	Wireless and Mobile Networks – Wi-Fi, Cellular Networks, Bluetooth	
	4	Cloud Networking Basics – Virtualization, Data Centers, SDN	
	5	Emerging Trends – IoT, 5G Networks, Network Automation	

5	**Teacher Specific Module**	
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	12

Essential Readings:

1. Tanenbaum, Andrew S., and David J. Wetherall. *Computer Networks*. 5th ed., Pearson, 2011.
2. Stallings, William. *Data and Computer Communications*. 10th ed., Pearson, 2013.
3. Forouzan, Behrouz A. *Data Communications and Networking*. 5th ed., McGraw Hill, 2012.
4. Stallings, William. *Network Security Essentials: Applications and Standards*. 6th ed., Pearson, 2017.

Suggested Readings:

1. KUrose, James F., and Keith W. Ross. *Computer Networking: A Top-Down Approach*. 7th ed., Pearson, 2017.
2. Schneier, Bruce. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. 2nd ed., Wiley, 1996.

Assessment Rubrics:

Evaluation Type		**Marks**
End Semester Evaluation		**70**
Continuous Evaluation		**30**
a)	Test Paper- 1	5
b)	Model Examination	10
c)	Assignment- 2 Numbers	10
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
Total		**100**

KU3DSCCSY203: PROGRAMMING IN JAVA

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
3	DSC	200-299	**KU3DSCCSY203**	4 (3T+1P)	75

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
3	2	-	35	65	100	1.5Hrs

Course Description:

Java is a multi-platform, object-oriented, and network-centric language that can be used as a platform in itself. It is a fast, secure, reliable programming language for coding everything from mobile apps and enterprise software to big data applications and server-side technologies.

Course Prerequisite: NIL

Course Outcomes:

CO No.	Expected Outcome	Learning Domains
1	Demonstrate proficiency in fundamental Object-Oriented Programming (OOP) concepts.	U, A
2	Implement multithreading, synchronization, and advanced exception handling techniques in Java, showcasing the ability to handle concurrent programming challenges.	U, A
3	Develop AWT applications, applying event handling mechanisms and utilizing appropriate layout managers for effective GUI design	U, A

4	Develop Swing applications with interactive user interfaces	U, A
5	Use Java Database Connectivity (JDBC) to interact with databases	U, A

*****Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)***

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	3			2			
CO 2		2					
CO 3	3	3					
CO 4	2	3					3
CO 5	3	3		2			3

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	**UNIT**	**DESCRIPTION**	**HOURS**
1	**MODULE 1: Introduction to OOP and Java Basics**		
	1	Understanding Object-Oriented Programming (OOP) Concepts - Introduction to Classes and Objects - Encapsulation, Inheritance, Polymorphism, and Abstraction.	15
	2	Introduction to Java - Overview of Java Programming Language – Setting up the Java Development Environment (IDE)-Basic Syntax and Data Types in Java.	
	3	Control Flow and Looping Constructs: if statements, switch statement,	
	4	Looping statements, jumping statements	

2	**MODULE 2: Java Inheritance and interfaces**		
	1	Introducing Classes: Class fundamentals; Introducing methods; Declaring Objects; Constructors	15
	2	This keyword; Garbage collection; the finalize method.	
	3	Inheritance basics - Types of inheritance. using super keyword-Method Overriding; Dynamic method dispatch; Abstract classes.	
	4	Packages and interfaces-creating a package-CLASSPATH-simple program using packages; interfaces-definition-extending interface-implementing interface- simple program using interface	

3	**MODULE 3: GUI Programming with AWT**		
	1	Multithreading in Java -Understanding Threads and Concurrency-Synchronization and Thread Safety-Thread life cycle.	15
	2	Exception Handling: try and catch , multiple catch-finally-nested try-throw-user defined exception.	
	3	Introduction to Abstract Window Toolkit: Basic Classes in AWT: Graphics, Colours, Font, Frame. Scroll bars.	
	4	AWT controls -Labels, Buttons, Checkbox, Radio buttons, Choice control, List, Text box,	

4	**MODULE 4: Advanced GUI Programming with Swing**		
	1	Event handling: event listeners: ActionListener, Item Listener, TextListener, MouseListener, Create a sample GUI application using Frame and AWT controls.	15
	2	Layout Managers: FlowLayout,BorderLayout, GridLayout, CardLayout, Implementing Menus Introduction to Swing: Swing packages, swing components and containers, Creating Swing GUI using JFrame.	
	3	Swing components: JLabel, JButton, JCheckBox, JRadioButton, JList, JComboBox, JTextFiled, JTextArea	

	4	Java Database Connectivity (JDBC)- Connecting to Databases with JDBC- Executing SQL Queries and Handling Result Sets	

5	**Teacher Specific Module**	
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	15

Essential Readings:

1. Sierra, Kathy, and Bert Bates. *Head First Java*. 3rd ed., O'Reilly Media, 2022.
2. Schildt, Herbert. *Java: The Complete Reference*. 11th ed., Oracle Press/McGraw Hill, 2019.
3. Radha Krishna, P. *Object Oriented Programming through Java*. Universities Press, 2007.

Suggested Readings:

1. Martin, Robert C. *Clean Code: A Handbook of Agile Software Craftsmanship*. Prentice Hall, 2008.
2. Oaks, Scott, and Henry Wong. *Java Threads*. 2nd ed., O'Reilly Media, 1999.

Assessment Rubrics:

Evaluation Type	**Marks**
End Semester Evaluation	**50 (Theory)** **15 (Practical)**
Continuous Evaluation	**35**
CE (Theory)	**25**

a)	Test Paper- 1	5
b)	Model Exam	10
c)	Assignment(2 numbers)	5
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
CE (Practical)		**10**
Total		**100**

KU3VACCSY201: CYBER LAWS AND RULES

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
3	VAC	200-299	**KU3VACCSY201**	3	45

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
3	0	-	25	50	75	1.5 hrs.

Course Description:

Cyber Laws and Rules is an essential course that introduces the legal and regulatory aspects of cyberspace. It focuses on the Information Technology Act, digital evidence, data privacy, cybercrimes, intellectual property rights, and international cyber law frameworks. This course enables students to understand the rights, responsibilities, and legal remedies in the digital environment without needing prior legal expertise.

Course Prerequisite: NIL

Course Outcomes:

CO No.	Expected Outcome	Learning Domains
1	Understand the key concepts and terminologies in cyber law and information technology legislation.	U
2	Identify legal issues related to cybercrime, privacy, and intellectual property in cyberspace.	U, An
3	Analyze the provisions of the IT Act, 2000, and other relevant Indian laws.	An
4	Evaluate legal procedures for handling digital evidence and cybercrime investigations.	E

****Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)***

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	3	3	2	2			
CO 2	3	3	2	2			
CO 3	3	3	2	2			
CO 4	3	3	2	2			

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	UNIT	DESCRIPTION	HOURS
1	**MODULE 1:** INTRODUCTION		
	1	Origin and meaning of Cyberspace;-Cyberspace vs. Physical space; Legal Issues in Cyberspace;	12
	2	Need of Regulation for Cyberspace; Different Models of Cyberspace Regulation	
	3	Cyber jurisdiction - Concept of Jurisdiction - Jurisdiction in Cyberspace	
	4	Issues and concerns of Cyberspace Jurisdiction in India	
2	**MODULE 2:** INFORMATION TECHNOLOGY ACT		
	1	A brief overview of Information Technology Act, 2000 - IT Act 2000 vs. IT Amendment Act 2008 -	9
	2	Relevant provisions from Indian Penal Code, Indian Evidence Act, Bankers Book Evidence Act, Reserve Bank of India Act.	
	3	Technological Concept of electronic signature and digital signature - Relevance of Signature - Handwritten signature vs Digital Signature Technological Advancement and development of signature -Digital Signature: IT Act, 2000	

	4	UNCITRAL Model Law on Electronic Signature	

3	**MODULE 3:** DATAPROTECTION AND PRIVACY CONCERNS IN CYBERSPACE		
	1	Need to protect data in cyberspace - Types of data - Legal framework of data protection - GDPR	9
	2	Concept of privacy- Privacy concerns of cyberspace- Constitutional framework of privacy - Judicial interpretation of privacy in India.	
	3	Concept of Electronic Records and Electronic Evidence - Recognition of electronic records under the UNCITRAL Model Law & ITAct.	
	4	Types of Electronic Evidence-Sources of electronic evidence Technical Issues in collection of electronic Evidence.	

4	**MODULE 4:** IP PROTECTION ISSUES IN CYBERSPACE		
	1	Copyright issues in cyberspace-Fundamental notions of copyright law - Copyright issues in cyberspace -Indian legal protection of copyright in cyberspace & concept of DRM	9
	2	Trademark issues in cyberspace-Meaning, Purpose and Kinds of Domain Name- Domain Name Vs Trademark - Domain Name Registration, ICANN, - Domain Name dispute and Related Laws	
	3	Patent issues in cyberspace--new emerging issues of cyberspace -	
	4	Cloud Computing, -Big Data - Internet of Things -Artificial Intelligence and Robotics –Blockchain.	

5	**Teacher Specific Module**	
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	9

Essential Readings:

1. Chris Reed, Internet Law-Text and Materials, Universal Law Publishing Co., New Delhi, 2nd Edition, 2005
2. Ian J Lloyd, Information Technology Law, Oxford University Press, 7th Edition, 2014
3. Nandan Kamath, Law Relating to Computers Internet & E Commerce Universal Law Publisher, 5th Edition, (2012)
4. Aparna Viswanathan, Cyber Law Indian and International Perspectives, Lexis Nexis, 2012
5. Karnika Seth, Computers, Internet and New Technology Laws-A comprehensive reference work with special focus on developments in India. Lexis Nexis, Updated Edition 2016
6. Anirudh Rastogi, Cyber Law, Lexis Nexis, 2014
7. Pavan Duggal Cyber Law 3.0, Universal Law Publishing Company Private Limited, 2014 Edition.
8. Talat Fatima, Cybercrimes, Eastern Book Company, Lucknow, Second Edition, 2016

Assessment Rubrics:

Evaluation Type		**Marks**
End Semester Evaluation		**50**
Continuous Evaluation		**25**
a)	Test Paper- 1	5
b)	Model exam	10
c)	Assignment	5
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
Total		**75**

KU4DSCCSY204: WEB TECHNOLOGY AND WEB SECURITY

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
4	DSC	200-299	**KU4DSCCSY204**	4 (3T+1P)	75

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
3	2		35	65	100	1.5hrs.

Course Description:

Web technology refers to the means by which computers communicate with each other using mark-up languages and multimedia packages. It gives us a way to interact with hosted information, like websites. Web technology involves the use of hypertext mark-up language (HTML).

Course Prerequisite: NIL

Course Outcomes:

CO No.	Expected Outcome	Learning Domains
1	Discuss various components in web technology.	U
2	Use HTML Forms in documents.	U,A
3	Design a web document with server-side scripting using PHP.	U, A,C
4	Identify the basics of Web Application Security.	U

****Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)***

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	3			2			

CO 2	3		2				
CO 3	3	3	3	2			
CO 4	3	2	2	2		2	2

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	UNIT	DESCRIPTION	HOURS
1	**MODULE 1:Introduction to HTML**		
	1	Introduction to HTML, Editing HTML5, W3C HTML5 Validation Service, Headings, Linking, Images, Special Characters and Horizontal Rules	15
	2	Lists, Tables, Forms, HTML5 Form Input types, input and data list 15 Elements and autocomplete Attribute, Frames and frameset	
	3	Web hosting, Types of web hosting, Hosting Space	
	4	Domain Name Registration, Free Hosting, Responsive Web designing	
2	**MODULE 2:Introduction to JavaScript**		
	1	Introduction to JavaScript , operators	15
	2	Arrays-declaring and allocating arrays, examples using arrays	
	3	Functions-Function Definitions -Defined Functions, scope rules and recursion.	
	4	Document Object Model, Objects-math, string and date objects, dialog boxes.	
3	**MODULE 3: PHP**		
	1	Introduction to PHP , Basic Syntax, Defining variable and Constants, Php Data type, Operator and Expression	15
	2	Function, Define a function, Array -Creating index based and Associative array Accessing array	
	3	Looping with associative array using each () and foreach(), Handling Html Form with Php Capturing Form.	

	4	Working with database.	

4	**MODULE 4: Web Application Security**		
	1	OWASP Top 10 Web Vulnerabilities – SQL Injection, OS Command, XSS, XML Injection	
	2	Cross-Site Request Forgery, Cookie Stealing, Broken Access Control	
	3	Session Hijacking, API Security (with Postman), Data Tampering	
	4	Web Attacks: Application Layer DoS/DDoS, File Path Traversal	

5	**Teacher Specific Module**	
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	15

Essential Readings:

1. Deitel, Paul J., Harvey M. Deitel, and Abbey Deitel. *Internet & World Wide Web: How to Program*. 5th ed., Pearson, 2011.
2. Meloni, Julie C. *Sams Teach Yourself HTML and CSS in 24 Hours*. 9th ed., Sams Publishing, 2018.
3. Flanagan, David. *JavaScript: The Definitive Guide*. 7th ed., O'Reilly Media, 2020.
4. Nixon, Robin. *Learning PHP, MySQL & JavaScript: With jQuery, CSS & HTML5*. 6th ed., O'Reilly Media, 2021.

Assessment Rubrics:

Evaluation Type		**Marks**
End Semester Evaluation		**50 (Theory)** **15 (Practical)**
Continuous Evaluation		**35**
CE (Theory)		**25**
a)	Test Paper- 1	5
b)	Model Exam	10

c)	Assignment(2 numbers)	5
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
CE (Practical)		**10**
Total		**100**

KU4DSCCSY205: FUNDAMENTALS OF CYBER SECURITY

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
4	DSC	200-299	**KU4DSCCSY205**	4 (3T+1P)	75

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
3	2	-	35	65	100	1.5 hrs.

Course Description:

This course provides an overview of the principles and practices of cyber security. Students will learn about the fundamental concepts of Network securities, common threats and vulnerabilities, and strategies for protecting systems and data.

Course Prerequisite: NIL

Course Outcomes:

CO No.	Expected Outcome	Learning Domains
1	Understand the fundamental concepts of cyber security.	U
2	Identify various types of cyber threats and vulnerabilities.	U
3	Understand the relationship between AI technologies and cyber defense.	An
4	Implement security measures and best practices.	C

****Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)***

Mapping of Course Outcomes to PSOs

	PSO 1	**PSO 2**	**PSO 3**	**PSO 4**	**PSO 5**	**PSO 6**	**PSO 7**

CO1	3	2					
CO2	3	3					
CO3	2	3			3		
CO4	3	3		3	3	3	3

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	UNIT	DESCRIPTION	HOURS
1	**MODULE TITLE: Introduction to Cyber Security**		
	1	Introduction, Need for Cyber Security.	15
	2	Cyber Security terminology - Cyberspace, Cybercrime, Cyber-attack, Threat, Vulnerability, Malware, Phishing, Botnets, Adware, Denial of Service , Ransomware, Key Logger.	
	3	The CIA Triads- Confidentiality, Integrity and Availability. Consequences of Weak Security, Challenges in Cyber Security.	
2	**MODULE TITLE: Data and Information Security**		
	1	Data and Information, Data security concepts: confidentiality, integrity, and availability.	15
	2	Access control and authentication mechanisms, Encryption methods: symmetric vs. Asymmetric	
	3	Data loss prevention (DLP) and secure backups, Privacy and personal data protection (GDPR, Indian IT Act).	
3	**MODULE TITLE: Network Security Fundamentals**		
	1	Need for Network Security, Hacking, stages of Hacking, Ethical hacking.	15

	2	Types of Network attacks- Spoofing, Sniffing, Mapping, Hijacking, Trojans, DoS and DDoS.	
	3	Firewalls- Types of firewalls, intrusion detection/prevention systems (IDS/IPS).	

	MODULE TITLE: Artificial Intelligence and Cyber Security		
4	1	Overview of AI and its applications. Machine Learning Basics: Supervised, Unsupervised, Reinforcement Learning .	15
	2	Deep Learning: Neural Networks, CNNs, RNNs, Transformers.	
	3	AI Tools & Frameworks: Scikit-learn, TensorFlow, Keras, Pytorch.	
	4	Role of AI in threat detection and anomaly analysis, AI-based intrusion detection systems (IDS)	

5	**Teacher Specific Module**	**15**
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	

Essential Readings:

1. Agrawal, Narmrata. *Cyber Security: A Complete Solution*. Dreamtech Press, 2018.
2. Goutam, Rajesh KUmar. *Cybersecurity Fundamentals*. BPB Publications, 2021.
3. Graham, James, Ryan Olson, and Rick Howard, editors. *Cyber Security Essentials*. Auerbach Publications, 2010.

Assessment Rubrics:

Evaluation Type		**Marks**
End Semester Evaluation		**50 (Theory)** **15 (Practical)**
Continuous Evaluation		**35**
CE (Theory)		**25**
a)	Test Paper- 1	5
b)	Model Exam	10
c)	Assignment(2 numbers)	5
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
CE (Practical)		**10**
Total		**100**

KU4DSCCSY206: PYTHON PROGRAMMING

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
4	DSC	200-299	**KU4DSCCSY206**	4 (3T+1P)	75

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
3	2		35	65	100	1.5hrs.

Course Description:

Python Programming is a foundational course designed to equip students with essential programming skills using Python. Additionally, students will gain hands-on experience in Python database connectivity.

Course Prerequisite: NIL

Course Outcomes:

CO No.	Expected Outcome	Learning Domains
1	Understand and apply the fundamental concepts of Python programming.	U,A
2	Write Python programs using functions, control structures, and file operations.	A
3	Develop Python programs using object-oriented programming and libraries.	A,C
4	Develop the ability to connect Python with SQL databases and perform data operations using cursor methods and query execution.	A, C

**Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)*

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7

CO 1	3			2			
CO 2	3		2				
CO 3	3	3	3	2			
CO 4	3	2	2	2		2	2

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	**UNIT**	**DESCRIPTION**	**HOURS**
1	**MODULE 1: Python Programming Basics**		
	1	Introduction to Python – Features, Variables, Data Types – int, float, str, bool, type conversion, mutable and immutable data types, Indentation, Comments, keywords.	15
	2	Input/Output, Basic Operators, Expressions.	
	3	Decision control flow statements– if, if-else, if..elif..else, nested if, Loops – while, for, continue and break statements.	
	4	Exception- Syntax error, Exception, Exception handing using try…. except…. Finally.	

2	**MODULE 2: Functions, Strings, Lists, Dictionaries, Tuples and sets**		
	1	Functions and Strings – function definition, calling the function, return statements, parameters, and scope of variables. Strings – Creating and storing strings, accessing characters in string by index number, slicing, string traversing, built-in functions, string Methods.	15
	2	List-List operations - creating, initializing, Indexing and slicing, traversing and manipulating lists, list methods and built-in functions, nested lists, list as argument to a function.	
	3	Dictionaries- Concept of key-value pair, mutability, creating, initializing, traversing, updating and deleting elements; dictionary methods and built-in functions.	

	4	Tuples and Sets- Tuples: Creating, initializing, accessing elements, tuple assignment, operations on tuples, tuple methods and built-in functions, nested tuples, Tuple packing and unpacking, Set methods.	

3	**MODULE 3: Files and Pandas libraries**		
	1	Files- Types of Files, Text file and binary file, open and close files, reading and writing text files, file access modes. File paths, CSV file: import csv module, open / close csv file, write into a csv file using csv. writerow() and read from a csv file using csv.reader( )The pickle module.	15
	2	Introduction to Pandas libraries- Introduction to pandas. Data structures in Pandas - Series and Data Frames.	
	3	Series: Creation of Series from – ndarray, dictionary, scalar value; mathematical operations; Head and Tail functions; Selection, Indexing and Slicing.	
	4	Data Frames: creation - from dictionary of Series, list of dictionaries, Text/CSV files; display; iteration; Operations on rows and columns: add, select, delete, rename; Head and Tail functions; Indexing using Labels, Boolean Indexing.	

4	**MODULE 4: Working with Databases (Database Connection)**		
	1	Interface of python with an SQL database: connecting SQL with Python.	15
	2	Performing insert, update, delete queries using cursor	
	3	Display data by using fetchone(), fetchall(), rowcount,	
	4	Creating database connectivity applications	

5	**Teacher Specific Module**	
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	15

Essential Readings:

1. Gowrishankar, S., and Veena A. *Introduction to Python Programming*. CRC Press, 2018.
2. Thareja, Reema. *Python Programming*. Oxford University Press, 2017.
3. Kamthane, Ashok Namdev, and Amit Ashok Kamthane. *Programming and Problem Solving with Python*. McGraw Hill, 2017.
4. Balagurusamy, E. *Introduction to Computing and Problem Solving Using Python*. McGraw Hill, 2016.
5. Hameed, Mohd Abdul. *Python for Data Science*. Wiley India Pvt. Ltd., 2018.
6. O'Connor, T. J. *Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers*. Syngress, 2012.

Assessment Rubrics:

<table>
<tr><td colspan="2">Evaluation Type</td><td>Marks</td></tr>
<tr><td colspan="2">End Semester Evaluation</td><td>50 (Theory)
15 (Practical)</td></tr>
<tr><td colspan="2">Continuous Evaluation</td><td>35</td></tr>
<tr><td colspan="2">CE (Theory)</td><td>25</td></tr>
<tr><td>a)</td><td>Test Paper- 1</td><td>5</td></tr>
<tr><td>b)</td><td>Model Exam</td><td>10</td></tr>
<tr><td>c)</td><td>Assignment(2 numbers)</td><td>5</td></tr>
<tr><td>d)</td><td>Seminar</td><td rowspan="4">5</td></tr>
<tr><td>e)</td><td>Book/ Article Review</td></tr>
<tr><td>f)</td><td>Viva-Voce</td></tr>
<tr><td>g)</td><td>Field Report</td></tr>
<tr><td colspan="2">CE (Practical)</td><td>10</td></tr>
<tr><td colspan="2">Total</td><td>100</td></tr>
</table>

KU4DSCCSY207: INFORMATION SECURITY

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
4	DSC	200-299	**KU4DSCCSY207**	4	75

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
4	0	-	30	70	100	2 hrs.

Course Description:

This course introduces fundamental information security principles, technologies, and practices. Students will learn about core security concepts (confidentiality, integrity, availability), identify modern cyber threats and attack methods, and apply basic cryptographic techniques. The course also covers network protocol security, web application vulnerabilities, and security best practices for operating systems, cloud, and IoT, with an introduction to incident response.

Course Prerequisite: Basic understanding of computer networks and fundamental knowledge of operating systems

Course Outcomes:

CO No.	Expected Outcome	Learning Domains
1	Understand core security principles and identify cyber threats, vulnerabilities, and attack methods.	U
2	Apply basic cryptographic techniques to secure data.	U, A, C
3	Evaluate network protocol security and recognize web application vulnerabilities.	U, A, An
4	Grasp security best practices for operating systems, cloud, and IoT,	U, E

	including incident response basics.	

Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1			3		3		2
CO 2	2	1	2			3	
CO 3			3		3		3
CO 4			2		2	3	3

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	UNIT	DESCRIPTION	HOURS
1	**MODULE 1: Information security Fundamentals & Threats**		
	1	Introduction to Information Security: Why security matters: Core Principles (CIA Triad, Authenticity, Non-repudiation).	15
	2	Modern Cyber Threats: Types of Malware (Viruses, Ransomware).Common Attack Methods (Phishing, DoS/DDoS, Social Engineering).Vulnerabilities.	
	3	Security Basics: Risk Management, Security Policies. Basic Controls (Firewalls, IDS/IPS).	

2	**MODULE 2: Symmetric Crypto & Hashing**		
	1	Traditional Symmetric Key Ciphers: Substitution Ciphers (e.g., Caesar Cipher, Playfair Cipher).Transposition Ciphers (e.g., Rail Fence Cipher).	15
	2	Symmetric Key Cryptography: Stream vs. Block Ciphers. Advanced Encryption Standard (AES): Simplified overview. Block Cipher	

		Modes: Common uses. Key Management basics	
	3	Cryptographic Hash Functions: Properties (One-way, Collision Resistance).Algorithms (SHA-256) and Uses (Data integrity, Password storage).	
	4	Message Authentication Codes (MACs): Purpose and HMAC.	

	MODULE 3: Asymmetric Crypto & PKI		
3	1	Asymmetric Key Cryptography (Public Key): • Public/private key concept and uses (Confidentiality, Digital Signatures, Key Exchange). • RSA Algorithm: Simplified overview. • Elliptic Curve Cryptography (ECC): Benefits. • Diffie-Hellman: Secure key exchange.	15
	2	Digital Signatures: How they work (Signing, Verification) and Benefits (Authentication, Integrity, Non-repudiation).	
	3	Public Key Infrastructure (PKI): Components (Digital Certificates, CAs), Certificate Revocation, Trust models.	

	MODULE 4: Network & Application Security		
4	1	Network Security Protocols: • Securing web traffic (TLS/SSL). • Securing Internet Protocol communications (IPSec). • Virtual Private Networks (VPNs). • Wireless Security (WPA2, WPA3)	15
	2	Web Application Security: OWASP Top 10 (Key Vulnerabilities): Injection, Broken Authentication, XSS, Security Misconfiguration, Sensitive Data Exposure, CSRF. Basic Secure Coding	
	3	Operating System Security: Access Control (DAC, MAC, RBAC).User authentication, Patching.	

5	**Teacher Specific Module**	

	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	15

Essential Readings:

1. William Stallings, *Cryptography and Network Security - Principles and Practice*, 8th Edition, Pearson. (Referred to as "Stallings")
2. Behrouz A. Forouzan and Debdeep Mukhopadhyay, *Cryptography And Network Security*, 3rd Ed, McGraw Hill. (Referred to as "Forouzan")

Assessment Rubrics:

Evaluation Type		**Marks**
End Semester Evaluation		**70**
Continuous Evaluation		**30**
a)	Test Paper- 1	5
b)	Model Exam	10
c)	Assignment(2 numbers)	10
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
Grand Total		**100**

KU4SECCSY201: LINUX SYSTEM AND NETWORK ADMINISTRATION

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
4	SEC	200-299	**KU4SECCSY201**	3 (2T+1P)	60

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
2	2	-	25	50	75	1.5hrs.

Course Description:

Linux System and Network Administration provides foundational knowledge of Linux system internals and basic networking principles. It introduces system boot mechanisms, user and file system administration, TCP/IP networking, and key server configurations. The course also explores process communication and basic socket programming. This practical-oriented subject equips students with essential system and network administration skills needed in modern IT environments.

Course Prerequisite: NIL

Course Outcomes:

CO No.	Expected Outcome	Learning Domains
1	Understand Linux booting processes and system configuration techniques.	U
2	Administer file systems, users, and essential system services securely.	A
3	Configure network settings and deploy basic network services.	A
4	Implement interprocess communication and write basic socket-based applications.	A, C

**Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)*

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	3			2			
CO 2	3		2				
CO 3	3	3	3	2			
CO 4	3	2	2	2		2	2

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	**UNIT**	**DESCRIPTION**	**HOURS**
1	**MODULE 1: Boot process and System Configuration**		
	1	Introduction: Important parts of kernel; Major services in a UNIX system: init, login from terminals, syslog , periodic command execution cron and at.	12
	2	**Boot process:** The LILO boot process: /etc/lilo.conf; The GRUB boot process.	
	3	Run levels: /etc/inittab, start-up script /etc/rc.d/rc.sysinit .	
	4	**System Configuration**: The /etc/sysconfig/… files, kernel modules.	
2	**MODULE 2: File system configuration**		
	1	File system types, /etc/fstab layout and meaning; Basic user environment: /etc/skel/… and home directories.	12
	2	**System Security:** Host security: tcp_wrappers and /etc/hosts.allow and /etc/hosts.deny.	
	3	File permissions, users groups and umask; Adding and deleting users-/etc/passwd and /etc/shadow files.	

	4	**System maintenance:** Syslogd, /etc/syslog.conf; The system crontab.	

3	**MODULE 3: Network Configuration**		
	1	TCP / IP Network Configuration: Introduction to TCP / IP network, Protocols, IP address, Hostname.	12
	2	Interface Configuration: loop back interface, Ethernet interface, Configuring Gateway, Network commands: ifconfig, netstat, route.	
	3	Network applications Configuration: File Transfer Protocol (FTP), Network File Systems (NFS) ,Network Information System(NIS),	
	4	Hyper Text Transfer Protocol (HTTP) and Web server, Server Message Block (SMB) Protocol and Samba server, Dynamic Host configuration Protocol (DHCP), Firewalls.	

4	**MODULE 4: DNS, IPC, and Socket Programming**		
	1	DNS Concepts, DNS database: SOA, NS, MX, A and PTR records, configuring DNS, Using nslooKUp.	12
	2	Introduction to IPC Mechanisms – fork(), pipe, message queue, semaphore, shared memory .	
	3	Socket Programming: Overview, Elementary Socket System Calls: socket(), bind(), connect(), listen(), accept(), send(), sendto() , recv() , recvfrom() , close() .	

5	**Teacher Specific Module**	
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	12

Essential Readings:

1. Nemeth, Evi et al. *UNIX and Linux System Administration Handbook, 4th Edition, Pearson, 2017*
2. Nemeth, Evi, Garth Snyder, Trent R. Hein, and Ben Whaley. *Linux Administration Handbook*. 2nd Edition, PHI Learning, 2009.
3. Hunt, Craig. *Linux DNS Server Administration*. BPB Publications, 2003.
4. Kirch, Olaf, and Terry Dawson. *Linux Network Administrator's Guide*. O'Reilly, 2003.
5. Stevens, W. Richard, Bill Fenner, and Andrew M. Rudoff. *UNIX Network Programming, Volume 1: The Sockets Networking API*. 3rd Edition, Addison-Wesley/PHI Learning, 2004.

Assessment Rubrics:

Evaluation Type		**Marks**
End Semester Evaluation		**35 (Theory)** **15 (Practical)**
Continuous Evaluation		**25**
CE (Theory)		**15**
a)	Test Paper- 1	5
b)	Model Exam	10
c)	Assignment(2 numbers)	5
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
CE (Practical)		**10**
Total		**75**

KU4VACCSY202: CYBER ETHICS

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
4	VAC	200-299	**KU4VACCSY202**	3	60

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
3	0		25	50	75	1.5hrs.

Course Description:

This course explores the ethical issues arising from the use of technology and the internet. It covers fundamental ethical concepts, decision-making frameworks, and the impact of technology on privacy, security, and intellectual property. Students will examine case studies and engage in discussions to develop critical thinking skills in ethical reasoning and apply them to real-world scenarios.

Course Prerequisite: NIL

Course Outcomes

CO No.	Expected Outcome	Learning Domains
1	Explain basic ethical principles and professional codes in cyber ethics.	U
2	Analyze privacy and security issues in the digital world.	An
3	Understand intellectual property rights and digital content usage.	U
4	Evaluate ethical challenges in social media and online behavior.	A, E
5	Assess ethical concerns in emerging technologies like AI	E

**Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)*

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	3			3			

CO 2	3			3		3	
CO 3				3		3	
CO 4				3		3	
CO 5				3	3		3

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	UNIT	DESCRIPTION	HOURS
1		**INTRODUCTION TO CYBER ETHICS**	**12**
	1	Ethical concepts and principles	
		Introduction to Cyber Ethics and Moral Theories	
		Ethical theories: Utilitarianism, Deontology, Virtue Ethics	
	2	Ethical decision-making frameworks	
		Steps in ethical decision-making, Ethical frameworks	
	3	Professional Ethics in Computing	
		Codes of ethics (ACM, IEEE, etc.)	
		Responsibilities of IT professionals	

2		**PRIVACY, SECURITY, AND SURVEILLANCE**	
	1	Privacy in the digital age: Data Collection, Profiling, and Behavioural Tracking	**12**
	2	Surveillance Technologies: Recording, Tracking, and Monitoring Techniques	
	3	Cybersecurity Threats: Viruses, Phishing, Ransomware	
	4	Ethical Dilemmas in Cybersecurity: Surveillance vs Rights, Whistle blowing	

	INTELLECTUAL PROPERTY	

3	1	Intellectual Property Rights	**12**
	2	Protecting Intellectual Property	
	3	Trade Secrets, Trademarks and Service Marks	
	4	Patents, Copyrights, Open access and open-source software	

4	**SOCIAL MEDIA AND EMERGING TECHNOLOGIES**		
	1	Ethics of Social Media	**12**
		Identity, Cyberbullying, Misinformation, Deepfakes	
	2	Ethics in Emerging Technologies	
		AI Ethics and Algorithmic Bias	
		Ethics in IoT and Cloud Computing	
	3	Ethics in Virtual and Augmented Reality (VR/AR)	
		Psychological Impact, Consent, and Manipulation of Reality	

5	**Teacher Specific Module**	**12**
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	

Essential Readings:

1. Tavani, H. T. (2018). Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing (5th ed.) John Wiley & Sons.
2. Quinn, M. J. (2014). *Ethics for the Information Age* (6th ed.). Pearson.
3. Baase, S., & Henry, T. – *A Gift of Fire: Social, Legal, and Ethical Issues for Computing Technology*
4. Himma, K. E., & Tavani, H. T. (2019). The Handbook of Information and Computer Ethics. John Wiley & Sons.

5. Johnson, D. G, Computer Ethics (4th ed.). Prentice Hall.

6. Computer network security and cyber ethics , Joseph Migga Kizza

Assessment Rubrics:

Evaluation Type		Marks
End Semester Evaluation		**50**
Continuous Evaluation		**25**
a)	Test Paper- 1	5
b)	Model exam	10
c)	Assignment	5
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
Total		**75**

KU4VACCSY203: FOSS FOR CYBER SECURITY

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
4	VAC	200-299	**KU4VACCSY203**	3	60

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
3	0	-	25	50	75	1.5hrs.

Course Description:

The Free and Open Source Software (FOSS) course is designed to familiarise students with the development process using free and open source software, which includes Linux operating system, service configuration management, application software, and development tools.

Course Prerequisite: NIL

Course Outcomes

CO No.	Expected Outcome	Learning Domains
1	State various FOSS concepts, features.	U
2	Discuss the features of Linux OS.	An
3	Execute Linux commands.	U
4	Demonstrate basic cyber security practices using FOSS platforms.	A, E

****Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)***

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	3			3			
CO 2	3			3		3	
CO 3				3		3	
CO 4				3		3	

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	UNIT	DESCRIPTION	HOURS
1	**MODULE 1: Open source software**		
	1	concepts, features, benefits over proprietary software, examples,	12
	2	Free software: concepts, features, advantages, Free software Vs Open Source software	
	3	Free and Open Source Software(FOSS), Fou essential freedoms	
	4	Free software movements, free software foundation(FSF),history, policies, GPL, free operating systems	
2	**MODULE 2: Linux**		
	1	Features, history, various Linux distributions,	12
	2	Linux architecture, kernel and shell-Linux desktop environments-GNOME and KDE.	
	3	Linux File System and Directories, types of files, Installing and Configuring Linux, File access permissions.	
3	**MODULE 3: Linux Commands**		
	1	Date, time, who, echo, man, info, cal, pwd, more, less, head, tail, chmod.	12
	2	mkdir, cd, cp, mv, rm, touch, sort, wc, cut, cat with options, ls with options , grep with options,	
	3	Mounting the file system, command line processing etc. Types of editors in Linux, Introduction to vi editor, modes in vi editor.	
	4	Commands for open a file, save a file, delete a file, quit a file etc.	
4	**MODULE 4: FOSS Tools for Cyber Security**		
	1	Network scanning and monitoring tools: Nmap, Wireshark	12
	2	Firewall configuration and security: Iptables, UFW	

	3	Basics of ethical hacking using open-source frameworks (OWASP ZAP, Metasploit Framework)	

5	**Teacher Specific Module**	
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	12

Essential Readings:

1. Negus, Christopher. *Red Hat Linux 9 Bible.* New Delhi: WILEY-Dreamtech, 2003.
2. Schenk, Thomas. *Red Hat Linux System Administration.* New Delhi: Techmedia, 2003.
3. *Kali Linux Revealed: Mastering the Penetration Testing Distribution.* Offensive Security.
4. Feller, Joseph, et al. *Perspectives on Free and Open Source Software.* MIT Press.

Assessment Rubrics:

Evaluation Type		**Marks**
End Semester Evaluation		**50**
Continuous Evaluation		**25**
a)	Test Paper- 1	5
b)	Model exam	10
c)	Assignment	5
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
Total		**75**

KU5DSCCSY301: ETHICAL HACKING

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
5	DSC	300-399	**KU5DSCCSY301**	4 (3T+1P)	75

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
3	2		35	65	100	1.5hrs.

Course Description:

The course enables students to learn ethical hacking and security challenges in computer networking. It addresses the data security issues, types of attacks including malwares, viruses, sniffer and denial of service. Students will also learn how to protect the network system using firewalls and filters, about the legal, professional and ethical issues.

Course Prerequisite: System and Network Security, Computer Networks.

Course Outcomes:

CO No.	Expected Outcome	Learning Domains
1	Explain the basic concepts of Ethical hacking.	U
2	Utilize the tools to conduct competitive intelligence and social engineering.	A
3	Examine the different types of cyber and network attack vectors and players.	A,C
4	Use different security techniques to protect system and user data.	A, C

****Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)***

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	3			2			

CO 2	3		2				
CO 3	3	3	3	2			
CO 4	3	2	2	2		2	2

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	UNIT	DESCRIPTION	HOURS
1	**MODULE 1:** Introduction to Ethical Hacking		
	1	Elements of Information Security, Authenticity and Non-Repudiation, Security Challenges,	15
	2	Effects of Hacking, Hacker – Types of Hacker, Ethical Hacker	
	3	Role of Security and Penetration Tester, Penetration Testing Methodologies :– OSSTMM, NIST, OWASP,	
	4	Categories of Penetration Test, Types of Penetration Tests, Vulnerability Assessment.	
2	**MODULE 2:** Foot Printing and Social Engineering		
	1	Tools for Foot Printing, Conducting Competitive Intelligence	15
	2	Google Hacking, Scanning, Enumeration, Trojans & Backdoors	
	3	Virus & Worms, Proxy & Packet Filtering, Denial of Service, Sniffer	
	4	Social Engineering–shoulder surfing, Dumpster Diving, Piggybacking.	
3	**MODULE 3:** Network attacks		
	1	Vulnerability Data Resources – Exploit Databases – Network Sniffing – Types of Sniffing – MITM Attacks – ARP Attacks	15
	2	Denial of Service Attacks - Hijacking Session with MITM Attack – DNS Spoofing – ARP Spoofing Attack Manipulating the DNS Records	
	3	DHCP Spoofing –Remote Exploitation – Attacking Network Remote Services	
	4	Overview of Brute Force Attacks – Traditional Brute Force – Attacking SMTP – Attacking SQL Servers – Testing for Weak Authentication.	

4	**MODULE 4:** Network Protection System & Hacking Web servers		
	1	Routers, Firewall & Honey pots, IDS &IPS, Web Filtering	15
	2	Vulnerability, Penetration Testing, Session Hijacking, Web Server	
	3	SQL Injection, Cross Site Scripting, Exploit Writing, Buffer Overflow, Reverse Engineering,	
	4	Email Hacking, Incident Handling & Response, Bluetooth Hacking, Mobiles Phone Hacking.	

5	**Teacher Specific Module**	
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	15

Essential Readings:

1. Michael T Simpson, Kent Back man, James Corley, "Hands on ethical hacking and network defense", Cengage Learning, 2nd edition, 2010.

2. Ed Skoudis and Tom Liston, "Counter Hack Reloaded: A step-by-step guide to computer attacks and effective defenses", Prentice Hall Series in Computer Networking and security, 2nd edition, 2006.
3. Rafay Baloch, "Ethical Hacking and Penetration Testing Guide", CRC Press, 2014.

Suggested Readings:

1. Kimberly Graves, "Certified Ethical Hacker: A Study Guide", Wiley Publishing, Inc., 2010.
2. Stuart Mc Clure, Joel Scambray, "Hacking Exposed 7 :Network Security Secrets & Solutions", McGraw-Hill publishing, edition 7, 2012

Assessment Rubrics:

Evaluation Type	**Marks**
End Semester Evaluation	**50 (Theory)** **15 (Practical)**

Continuous Evaluation		**35**
CE (Theory)		**25**
a)	Test Paper- 1	5
b)	Model Exam	10
c)	Assignment(2 numbers)	5
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
CE (Practical)		**10**
Total		**100**

KU5DSCCSY302: SYSTEM AND NETWORK SECURITY

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
5	DSC	300-399	**KU5DSCCSY302**	4 (3T+1P)	75

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
3	2		35	65	100	1.5hrs.

Course Description:

Study of this course provides the learners a clear understanding of the fundamental concepts of network and wireless security and the processes and means required to implement a secure network. It covers the techniques to transfer a message securely over insecure channel. This course covers the security measures in Windows and Linux operating systems. The course helps the learners to understand the various threats faced in the Internet and web services.

Course Prerequisite: Sound knowledge in Computer Networks.

Course Outcomes: After the completion of the course, the student will be able to

CO No.	Expected Outcome	Learning Domains
1	Explain the techniques for network protection and explore new tools and attacks in network security domain	U
2	Identify the challenges, attacks and defenses in Operating Systems.	A
3	Summarize the basic functionalities of Windows and Linux Hardening	A,C
4	Explain the various attacks as well as security in Internet and Web services.	A, C

****Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)***

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	3			2			
CO 2	3		2				
CO 3	3	3	3	2			
CO 4	3	2	2	2		2	2

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	**UNIT**	**DESCRIPTION**	**HOURS**
1	**MODULE 1: Principles of Network Security**		
	1	Network Security Terminologies, Network Security and Data Availability,	15
	2	Components of Network Security, Network Security Policies.	
	3	Network segments-Perimeter Defense, NAT, Basic architecture issues, Subnetting, Switching and VLANs,	
	4	Address Resolution protocol and media access control, Dynamic Host Configuration Protocol and Addressing Control.	
2	**MODULE 2: Windows Security**		
	1	Windows Security at the heart of the defense, Out-of the-box Operating system hardening,	15
	2	Installing applications, Putting the workstation on the network, Operating Windows safely,	
	3	Upgrades and Patches, Maintain and test the security, Attacks against the Windows workstation.	
	4	Linux Security- Physical security, Controlling the configuration, Operating Linux safely, Hardening Linux.	
3	**MODULE 3: Web Browser Security**		
	1	Web Browser and Client risk- How a web browser works, Web browser attacks, Operating safely,	15
	2	Web security- How HTTP works, Server and Client contents, State,	

		Attacking Web servers, Web Services.	
	3	E-mail security- The e-mail risk, Protocols, Authentication, Operating safely when using email,	
	4	Domain Name System – DNS basics, Purpose of DNS, Security Issues with DNS, DNS attacks.	

4	**MODULE 4: Network Security**		
	1	Security In Data Networks: Wireless Device security issues-GPRS security, GSM security, IP security.	15
	2	Wireless Transport Layer Security: Secure Socket Layer - Wireless Transport Layer Security - WAP Security Architecture - WAP Gateway.	
	3	Firewalls-types, rules, personal firewalls, Intrusion detection systems, responses to intrusion detection,	
	4	Penetration testing, Auditing and Monitoring.	

5	**Teacher Specific Module**	
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	15

Essential Readings:

1. Eric Cole, Ronald Krutz, James W. Conley, "Network Security Bible", First Edition Wiley India Pvt Ltd, 2010.
2. Michael A Whitman, Herbert J.Mattord, "Principles of Information Security", Cengage Learning, Fourth Edition, 2016.

Suggested Readings:

1. William Stallings, "Network Security Essentials",Pearson Education, 4th Edition, 2011
2. Eric Maiwald, "Fundamentals of Network Security", Tata McGraw-Hill, 2011

Assessment Rubrics:

Evaluation Type	**Marks**
End Semester Evaluation	**50 (Theory)** **15 (Practical)**

Continuous Evaluation		**35**
CE (Theory)		**25**
a)	Test Paper- 1	5
b)	Model Exam	10
c)	Assignment(2 numbers)	5
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
CE (Practical)		**10**
Total		**100**

KU5DSCCSY303: MALWARE FORENSICS

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
5	DSC	300-399	**KU5DSCCSY303**	4	75

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
4	0		30	70	100	2hrs.

Course Description:

The course enables the learners to understand malware forensics, use of manual and automated tools to analyze various malicious activity. During the course students will learn to identify and analyze various types of malware. It helps the learners to understand static and dynamic malware analysis techniques and malware behavior monitoring tools.

Course Prerequisite: Knowledge in Fundamental concepts of security.

Course Outcomes: After the completion of the course the student will be able to

CO No.	Expected Outcome	Learning Domains
1	Identify the nature of malware and its capabilities.	U
2	Explain the types of malware and different types of Malware analysis.	U
3	Identify the different malware detection techniques.	A,C
4	Explain the methods of data collection and examination in Windows and Linux Systems	A, C

**Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)*

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	3			2			

CO 2	3		2				
CO 3	3	3	3	2			
CO 4	3	2	2	2		2	2

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	UNIT	DESCRIPTION	HOURS
1	**MODULE 1: Introduction**		
	1	Introduction to malware, OS security concepts, malwarethreats, evolution of malware,	15
	2	Malware types - viruses,worms, rootkits,Trojans,bots, spyware, adware,logicbombs.	
	3	Types of malware Analysis – Static Analysis, Dynamic Analysis, Malware Analysis Techniques - Obfuscated, Deobfuscated,	
	4	Malware Analysis Tools - Static Analysis Tools, Dynamic Analysis Tools. AntivirusScanning, FingerprintforMalware.	
2	**MODULE 2: Malware Analysis**		
	1	Dynamic analysis: Live malware analysis, dead malware analysis, analyzing traces of malware system- calls, api-calls, registries, network activities.	15
	2	Anti-dynamic analysis techniques anti-vm, runtime-evasion techniques,	
	3	Malware Sandbox, Monitoring with Process Monitor, Packet Sniffing with Wireshark, Kernelvs.	
	4	User-Mode Debugging, OllyDbg, Breakpoints, Tracing, Exception Handling, Patching.	
	MODULE 3: Malware Detection		
	1	Malware Detection Techniques: Signature-based techniques: malware signatures, packed malware signature,	15
	2	metamorphic and polymorphic malware signature	
	3	Non-signature based techniques: similarity-based techniques,	

	4	Machine-learning methods, invariant inferences.	

4	**MODULE 4: Incident Response**		
	1	Malware Incident response: Volatile Data Collection and Examination on a Live Windows Systems - Volatile Data collection methodology from Windows systems- Preservation of Volatile data,	15
	2	Collecting Subject System details, Identifying users Logged into the System, Inspect Network Connections and Activity, Current and Recent Network Connections, Collecting Process Information,	
	3	Correlate Open Ports with Running Processes and Programs, Identifying Services and Drivers, Determining Scheduled Tasks, Collecting Clipboard Contents,	
	4	Non-Volatile Data Collection from a Live Windows System, Volatile Data collection methodology from Linux systems, Nonvolatile Data collection from a live Linux system.	

5	**Teacher Specific Module**	
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	15

Essential Readings:

1. James M.Aquilina, Cameron H.Malin ,Eoghan Casey,"Malware Forensics Field Guide for Windows Systems: Digital ForensicsFieldGuides",Syngress Publishing, First Edition,2012
2. JamesM.Aquilina,CameronH.Malin,EoghanCasey,"Malware ForensicsField Guide for LinuxSystems:Digital ForensicsField Guides",Syngress Publishing, Second Edition,2014
3. EoghanCasey,James M.Aquilina,CameronH.Malin,"Malware ForensicsInvestigatingandAnalyzingMalicious code",Syngress Publishing, First Edition,2008

Suggested Readings:

1.Michael Sikorski and Andrew Honig,"PracticalmalwareanalysisTheHands-OnGuide to Dissecting Malicious Software", No starch press, First Edition,2012.
2.Michael Davis,SeanBodmer, AaronLemasters,"Malware&rootkits:malware&rootkitssecurity secrets&Solutions",McGraw Hill,Second Edition,2010
3.VictorMarak,"WindowsMalwareAnalysisEssentials"PacktPublishing,First Edition, 2015

Assessment Rubrics:

Evaluation Type		Marks
End Semester Evaluation		**70**
Continuous Evaluation		**30**
a)	Test Paper- 1	5
b)	Model Exam	10
c)	Assignment(2 numbers)	10
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
Grand Total		**100**

KU5DSECSY301: DATABASE SECURITY

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
5	DSE	300-399	**KU5DSECSY301**	4 (3T+1P)	75

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
3	2		35	65	100	1.5hrs.

Course Description:

A Database Security course teaches the technical and administrative controls required to protect enterprise data from unauthorized access, modification, or breach.

Course Prerequisite: Nil

Course Outcomes:

CO No.	Expected Outcome	Learning Domains
1	Analyse various database models, design processes, and the ACID properties to evaluate their impact on data consistency and security.	U
2	Create advanced SQL queries, including secure practices to prevent SQL injection and ensure data integrity.	A
3	Compare and evaluate traditional RDBMS and NoSQL databases for handling structured, semi structured, and unstructured data	U
4	Apply access control mechanisms like Role.	A, C

****Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)***

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	3			2			

CO 2	3		2				
CO 3	3	3	3	2			
CO 4	3	2	2	2		2	2

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	UNIT	DESCRIPTION	HOURS
1	**MODULE 1:**		
	1	Different Types of Databases, Entity Relationship Models, Relational Models, Relational Algebra, Calculus,	15
	2	ACID Properties, Relational Databases, Concurrency Control, Process of Database Design,	
	3	Dependencies and Normalization for Relational Databases, Object oriented/Object-Relational Models, Threats to the Database,	
	4	Principles of Database Security, Levels of Database Security, Database Security Issues.	
2	**MODULE 2:**		
	1	Introduction to SQL, SQL Features, SQL Operators, SQL Datatypes, SQL Parsing, Types of SQL Commands,	15
	2	Advanced Study of Structured Query Language, Querying Data from the database, Correlated Sub-queries, Joins,	
	3	Hierarchical Queries, Bind Variables, Cursors, Functions, Stored Procedures,	
	4	MySQL, Basics of New SQL Databases, SQL Injection and Mitigation.	
3	**MODULE 3:**		
	1	Structured Data, Unstructured Data, Semi-Structured Data, Limitations of Traditional RDBMSs, SQL and Structured Data, SQL and Semi-Structured Data,	15
	2	SQL and Unstructured Data, The Emergence of NoSQL, NoSQL Database features, Types of NoSQL Databases, NoSQL Injection.	
	3	Search Engine Databases, Basics of MongoDB and Neo4j, Data Auditing, Statistical Database Security, Semantic Integrity Control,	

	4	Privilege Analysis, Virtual Private Database (VPD), Data Redaction, Sensitive Data Protection.	

4	**MODULE 4:**		
	1	Authentication and Authorization in DBMS, Properties and Basic Principles of Access Control Mechanisms, Views for Access Control, Classical Database Access Control: Discretionary Access Control,	15
	2	Role-Based Access Control and Mandatory Access Control; Access Control in Open Environments such as Attribute Based Encryption and Identity Based Encryption,	
	3	Access Control in SQL, Network Data Encryption, Strong Authentication, Private Data Aggregation,	
	4	Search in Encrypted Data: Searchable Encryption Overview, Selected Schemes on Searchable Encryption.	

5	**Teacher Specific Module**	
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	15

Essential Readings:

1. A.Silberschatz et al., Database System Concepts, 6th ed., McGraw-Hill, 2011.
2. A.Meier and M. Kaufmann, SQL and NoSQL Databases: Models, Languages, Consistency Options and Architectures for Big Data Management, Springer, 2019.
3. G. Harrison, Next Generation Databases: NoSQL, NewSQL, and Big Data, Apress, 2015.
4. R. Elmasri and S. B. Navathe, Fundamentals of Database Systems, 6th ed., Pearson Education, 2011.
5. R. B. Vatan, Implementing Database Security and Auditing, Digital Press, 1st ed., 2005.

Suggested Readings:

1. C. J. Date et al., An Introduction to Database Systems, 8th ed., Pearson Education, 2006.
2. R. Elmasri and S. Navathe, Fundamentals of Database Systems, Pearson, 2000.
3. G. K. Gupta, Database Management Systems, McGraw-Hill, 2011.

4. J. Hellerstein and M. Stonebraker, Readings in Database Systems (The Red Book), 4th ed., MIT Press, 2005.
5. J. L. Harrington, Object Oriented Database Design Clearly Explained, Harcourt, 2000.
6. R. Ramakrishnan, Database Management Systems, 4th ed., McGraw-Hill, 2015.
7. R. Ramakrishan and J. Gehrke, Database Management Systems, 3rd ed. McGraw-Hill, 2002.
8. S. Ceri and G. Pelagatti, Distributed Databases: Principles and Systems, Universities Press, 2000.
9. V. Atluri and P. Samarati, Security of Data and Transaction Processing, Springer, 2000.

Assessment Rubrics:

Evaluation Type		**Marks**
End Semester Evaluation		**50 (Theory)** **15 (Practical)**
Continuous Evaluation		**35**
CE (Theory)		**25**
a)	Test Paper- 1	5
b)	Model Exam	10
c)	Assignment(2 numbers)	5
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
CE (Practical)		**10**
Total		**100**

KU5DSECSY302: BLOCKCHAIN TECHNOLOGY

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
5	DSE	300-399	**KU5DSECSY302**	4	75

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
4	0		30	70	100	2hrs.

Course Description:

The purpose of this course is to create awareness and understanding among students on the foundation of blockchain technology. To learn the fundamentals of Blockchain and various types of block chain and consensus mechanisms.

Course Prerequisite: Knowledge in Computer Networks

Course Outcomes:

CO No.	Expected Outcome	Learning Domains
1	Understanding concepts behind crypto currency	U
2	Applications of smart contracts in decentralized application development	A
3	Understand frameworks related to public, private and hybrid blockchain	U
4	Create blockchain for different application case studies	A, C

****Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)***

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	3			2			
CO 2	3		2				
CO 3	3	3	3	2			

CO 4	3	2	2	2		2	2

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	UNIT	DESCRIPTION	HOURS
1	**MODULE 1: Fundamentals of Blockchain**		
	1	Fundamentals of Blockchain: Introduction, Origin of Blockchain, Blockchain Solution, Components of Blockchain, Block in a Blockchain, The Technology and the Future.	15
	2	Blockchain Types and Consensus Mechanism: Introduction, Decentralization and Distribution, Types of Blockchain, Consensus Protocol.	
	3	Cryptocurrency –, Cryptocurrency Basics, Types of Cryptocurrencies, Cryptocurrency Usage.	
	4	Bitcoin, Altcoin and Token: Introduction, Bitcoin and the Cryptocurrency.	
2	**MODULE 2: Public and Private Blockchain System**		
	1	Public Blockchain System: Introduction, Public Blockchain, Popular Public Blockchains,.The Bitcoin Blockchain, Ethereum Blockchain.	15
	2	Smart Contracts: Introduction, Smart Contract, Characteristics of a Smart Contract, Types of Smart Contracts. Types of Oracles, Smart Contracts in Ethereum, Smart Contracts in Industry.	
	3	Private Blockchain System: Introduction, Key Characteristics of Private Blockchain, Need of Private Blockchain, Private Blockchain Examples, Private Blockchain and Open Source,	
	4	E- commerce Site Example, Various Commands (Instructions) in E-commerce Blockchain, Smart Contract in Private Environment, State Machine, Different Algorithms of Permissioned Blockchain, ByzantineFault, Multichain.	
3	**MODULE 3:** Consortium Blockchain		
	1	**C**onsortium Blockchain : Introduction, Key Characteristics of Consortium Blockchain, Need of Consortium Blockchain,	15
	2	Hyperledger Platform, Overview of Ripple, Overview of Corda.	

	3	Initial Coin Offering: Introduction, Blockchain Fundraising Methods, Launching an ICO, Investing in an ICO,	
	4	Pros and Cons of Initial Coin Offering, Successful Initial Coin Offerings, Evolution of ICO, ICO Platforms.	

4	**MODULE 4: Security in Blockchain**		
	1	Introduction, Security Aspects in Bitcoin, Security and Privacy Challenges of Blockchain in General, Performance and Scalability, Identity Management and Authentication,	15
	2	Regulatory Compliance and Assurance, Safeguarding Blockchain Smart Contract (DApp), Security Aspects in Hyperledger Fabric.	
	3	Applications of Blockchain: Introduction, Blockchain in Banking and Finance, Blockchain in Education, Blockchain in Energy, Blockchain in Healthcare, Blockchain in Real-estate, Blockchain In Supply Chain,	
	4	The Blockchain and IoT. Limitations and Challenges of Blockchain.	

5	**Teacher Specific Module**	
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	15

Essential Readings:

1. “Blockchain Technology”, Chandramouli Subramanian, Asha A. George, Abhilasj K A and Meena Karthikeyan, Universities Press.

Suggested Readings:

1. Michael Juntao Yuan, Building Blockchain Apps, Pearson, India.
2. Blockchain Blueprint for Economy, Melanie Swan, SPD O'reilly.
3. Blockchain for Business, Jai Singh Arun, Jerry Cuomo, Nitin Gaur, Pearson.

Assessment Rubrics:

Evaluation Type	Marks
End Semester Evaluation	**70**

Continuous Evaluation		**30**
a)	Test Paper- 1	5
b)	Model Exam	10
c)	Assignment(2 numbers)	10
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
Grand Total		**100**

KU5SECCSY301: BIOMETRIC SECURITY

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
5	SEC	300-399	**KU5SECCSY301**	3	45

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
3	0	-	25	50	75	1.5 hrs

Course Description:

This course basically aims at imparting fundamental knowledge about concepts and the applications of biometric security. The course also aims at understanding of the techniques, algorithms and applications developed for biometrics and how it can be applied to solve real problems.

Course Prerequisite: NIL

Course Outcomes: After the completion of the course, the student will be able to

CO No.	Expected Outcome	Learning Domains
1	Summarize the fundamental concepts and performance measures in the basic type of biometric systems.	U
2	Recognize fingerprint patterns and trace how it can be effectively used in applications.	A
3	Identify Facial patterns and locate how it can be effectively used in Applications.	A,C
4	Acquire and detect iris and ear images and interpret its properties.	A, C

****Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)***

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	3			2			
CO 2	3		2				

CO 3	3	3	3	2			
CO 4	3	2	2	2		2	2

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	UNIT	DESCRIPTION	HOURS
1	**MODULE 1: Biometric fundamentals**		
	1	Biometric fundamentals – Biometric technologies – Biometrics Vs traditional techniques - Characteristics of a good biometric system	9
	2	Benefits of biometrics - Key biometric processes: verification, identification and biometric matching	
	3	Performance measures in biometric systems, FAR, FRR, FTE rate, EER and ATV rate,	
	4	Applications of Biometric Systems, Security and Privacy Issues, Physiological Biometrics and Behavioral Biometrics.	
2	**MODULE 2: Fingerprint and Face Recognition**		
	1	Fingerprint recognition: Friction ridge patterns, Acquisition,	9
	2	Feature extraction, matching, indexing, synthesis, palm print.	
	3	Face recognition: Introduction, image acquisition, face detection. Feature extraction of face recognition, matching, heterogeneous face recognition.	
	4	Signature-scan, Keystoke Scan– components, working principles.	
3	**MODULE 3: Iris and Ear Recognition**		
	1	Iris recognition, Image acquisition, iris segmentation, normalization.	9
	2	Encoding and matching, quality assessment, performance evaluation	
	3	Ear detection and recognition – challenges, gait and hand geometry.	

		Feature extraction and matching	

4	**MODULE 4: Security of Biometric Systems**		
	1	Security of bio-metric systems: adversary attacks, attacks on user interface,	9
	2	Attacks on bio-metric processing, database attacks.	
	3	Biometric standards, biometric databases.	

5	**Teacher Specific Module**	
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	9

Essential Readings:

1. Anil K. Jain, Arun A. Ross, Karthik Nandakumar, "Introduction to Biometrics", Springer, 2011
2. Jain, P. Flynn, A. Ross, "Handbook of Biometrics" Springer, 2008

Suggested Readings:

1. John R. Vacca, "Biometric Technologies and Verification Systems", Elsevier, 2007
2. Samir Nanavati, Michael Thieme, Raj Nanavati, "Biometrics – Identity Verification in a Networked World", Wiley-dreamtech India Pvt Ltd, New Delhi, 2003
3. Paul Reid, "Biometrics for Network Security", Pearson Education, New Delhi, 2004

Assessment Rubrics:

Evaluation Type		**Marks**
End Semester Evaluation		**50**
Continuous Evaluation		**25**
a)	Test Paper- 1	5
b)	Model exam	10
c)	Assignment	5

d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
Total		**75**

KU6DSCCSY304: VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
6	DSC	300-399	**KU6DSCCSY304**	4 (3T+1P)	75

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
3	2		35	65	100	1.5hrs.

Course Description:

A Vulnerability Assessment and Penetration Testing course teaches you to evaluate an organization's security posture by identifying, analyzing, and simulating cyberattacks on IT infrastructure. Give an introduction to Vulnerability Assessment and Penetration Testing.

Course Prerequisite: Knowledge in information security and Web Application

Course Outcomes:

CO No.	Expected Outcome	Learning Domains
1	Learn to handle the vulnerabilities of a Web application	U, A
2	Able to learn various penetration testing tools.	A
3	Knowledge on Metasploit, Linux exploit and windows exploit tools	A,C
4	Analyze various vulnerabilities	A, C

**Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)*

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	3			2			

CO 2	3		2				
CO 3	3	3	3	2			
CO 4	3	2	2	2		2	2

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	UNIT	DESCRIPTION	HOURS
1	**MODULE 1: Penetration Testing and Tools**		
	1	Introduction: Vulnerability Assessment and Penetration Testing.	15
	2	Ethics of Ethical Hacking: Why you need to understand your enemy's tactics, recognizing the gray areas in security,	
	3	Penetration Testing and Tools: Social Engineering Attacks: How a social engineering attack works, conducting a social engineering attack,	
	4	Common attacks used in penetration testing, preparing yourself for face-to-face attacks, defending against social engineering attacks.	
2	**MODULE 2: Physical Penetration Attacks**		
	1	Physical Penetration Attacks: Why a physical penetration is important? Conducting a physical penetration, Common ways into a building, defending against physical penetrations.	15
	2	Insider Attacks: Conducting an insider attack, defending against insider attacks.	
	3	Metasploit: The Big Picture, Getting Metasploit, Using the Metasploit Console to Launch Exploits, Exploiting Client-Side Vulnerabilities with Metasploit,	
	4	Penetration Testing with Metasploit's Meterpreter,Automating and Scripting Metasploit, Going Further with Metasploit.	
3	**MODULE 3: Managing a Penetration Test**		
	1	Managing a Penetration Test: planning a penetration test, structuring a penetration test, execution of a penetration test,	15
	2	Information sharing during a penetration test, reporting the results of a Penetration Test.	

	3	Basic Linux Exploits: Stack Operations, Buffer Overflows, Local Buffer Overflow Exploits, ExploitDevelopment Process.	
	4	Windows Exploits: Compiling and Debugging Windows Programs, Writing Windows Exploits, Understanding Structured Exception Handling (SEH), Understanding Windows Memory Protections (XPSP3, Vista, 7 and Server 2008), Bypassing Windows Memory Protections.	

4	**MODULE 4: Web Application Security Vulnerabilities**		
	1	Web Application Security Vulnerabilities: Overview of top web application security vulnerabilities, Injection vulnerabilities,	15
	2	Cross-Site scripting vulnerabilities, the rest of the OWASP Top Ten SQL Injection vulnerabilities, Cross-site scripting vulnerabilities.	
	3	Vulnerability Analysis: Passive Analysis, Source Code Analysis, Binary Analysis.	
	4	Malware Analysis: Collecting Malware and Initial Analysis: Malware, Latest Trends in Honeynet Technology, Catching Malware: Setting the Trap, Initial Analysis of Malware.	

5	**Teacher Specific Module**	
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	15

Essential Readings:

1. Gray Hat Hacking-The Ethical Hackers Handbook", Allen Harper, Stephen Sims, Michael Baucom, 3rd Edition, Tata Mc Graw-Hill.
2. The Web Application Hacker's Handbook-Discovering and Exploiting Security flaws", Dafydd Suttard, Marcus pinto, 1st Edition, Wiley Publishing.

Suggested Readings:

1. "Penetration Testing: Hands-on Introduction to Hacking", Georgia Weidman, 1st Edition, No Starch Press.
2. The Pen Tester Blueprint-Starting a Career as an Ethical Hacker ", L. Wylie, Kim Crawly, 1st Edition, Wiley Publications.

Assessment Rubrics:

Evaluation Type		**Marks**
End Semester Evaluation		**50 (Theory)** **15 (Practical)**
Continuous Evaluation		**35**
CE (Theory)		**25**
a)	Test Paper- 1	5
b)	Model Exam	10
c)	Assignment(2 numbers)	5
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
CE (Practical)		**10**
Total		**100**

KU6DSCCSY305: CYBER FORENSIC

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
6	DSC	300-399	**KU6DSCCSY305**	4	75

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
4	0		30	70	100	2hrs.

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 Prerequisite: NIL

Course Outcomes:

CO No.	Expected Outcome	Learning Domains
1	Understand fundamentals of cyber forensic, learn investigation tools and techniques, analysis of data to identify evidence.	U
2	Explain how to conduct a digital forensics investigation and how to report findings from digital forensic investigations using various forensic tools.	A
3	Accomplish the knowledge about Computer Forensics analysis and validation techniques.	A,C
4	Perform recovery of digital evidence from various digital devices using a variety of software utilities.	A, C

****Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)***

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	3			2			
CO 2	3		2				
CO 3	3	3	3	2			
CO 4	3	2	2	2		2	2

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	**UNIT**	**DESCRIPTION**	**HOURS**
1	**MODULE 1: Computer Forensics and Investigation**		
	1	Understanding computer forensics-Preparing for Computer Investigations	15
	2	Corporate High-Tech Investigation-Data Acquisition and Recovery	
	3	Storage Formats-Using acquisition tools	
	4	Data Recovery-RAID Data acquisition.	

2	**MODULE 2: Processing Crime and Incident Scene**		
	1	Identifying and collecting evidence-Preparation for search, Seizing and Storing Digital evidence.	15
	2	Computer Forensics tools (Encase)-Windows Operating System - Understanding file structure and file system	
	3	NTFS disks- Disk Encryption - Registry-Evidence Manipulation	
	4	Computer Forensics software and hardware tools-Chain of Custody-Handling digital evidence – best practices.	

3	**MODULE 3: Computer Forensics Analysis and Validation**		
	1	Data collection and analysis-Validation of forensics data-Data hiding technique	15

	2	Email Investigation and Mobile device Forensics	
	3	Investigation of e-mail crimes and Violations-Using specialized E-mail forensics tools	
	4	Understanding mobile device forensics and Acquisition procedures.	

4	**MODULE 4: Role of Digital Forensics in Real time applications**		
	1	SANS SIFT Investigative tool-PRO Discover Basic	15
	2	Volatility-Sleuth Kit-CAINE investigative environment Industry Trends	
	3	Forensics Standards-Introduction to Cloud Forensics	
	4	Introduction to IoT Forensics.	

5	**Teacher Specific Module**	
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	15

Essential Readings:

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.

Suggested Readings:

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: Threat scape and Best Practices" by John Sammons.

Assessment Rubrics:

Evaluation Type		Marks
End Semester Evaluation		**70**
Continuous Evaluation		**30**
a)	Test Paper- 1	5
b)	Model Exam	10
c)	Assignment(2 numbers)	10
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
Grand Total		**100**

KU6DSCCSY306: CLOUD SECURITY

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
6	DSC	300-399	**KU6DSCCSY306**	4	75

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
4	0		30	70	100	2hrs.

Course Description:

This course provides the ground-up coverage on the high level concepts of cloud landscape, architectural principles, techniques, design patterns and real-world best practices applied to Cloud service providers and consumers and delivering secure Cloud based services. The course also describes the Cloud security architecture and explores the guiding security design principles, design patterns, industry standards, applied technologies and addressing regulatory compliance requirements critical to design, implement, deliver and manage secure cloud based services.

Course Prerequisite: Operating System and Computer Networks

Course Outcomes: After the completion of the course, the student will be able to

CO No.	Expected Outcome	Learning Domains
1	Summarize core cloud computing concepts and fundamental principles, including standard delivery models and service designs.	U
2	Apprehend the foundational security practices that are required to secure modern cloud computing infrastructures.	A
3	Explain the standard cloud security network designs and architecture models.	A,C
4	Identify the industry security standards, regulatory mandates, audit policies and compliance requirements for Cloud based infrastructures	A, C

****Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)***

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	3			2			
CO 2	3		2				
CO 3	3	3	3	2			
CO 4	3	2	2	2		2	2

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	**UNIT**	**DESCRIPTION**	**HOURS**
1	**MODULE 1: Introduction to Cloud Computing**		
	1	Cloud Computing, NIST reference Model, Basic terminology and concepts, Cloud characteristics, benefits and challenges,	15
	2	Cloud delivery (service) models: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS),	
	3	Software-asaService (SaaS), XaaS (Anything-as-a-service),	
	4	Cloud deployment models: Public cloud, Community cloud, Private cloud, Hybrid cloud, Open Cloud Services.	
2	**MODULE 2: Fundamental Cloud Security**		
	1	Basic Terms and Concepts in Security,	15
	2	Threat Agents, Cloud Security Threats, Identity Management and Access Control,	
	3	Cloud Security Working Groups, Elements of Cloud Security Model,	
	4	Cloud Security Reference Model, Examining Cloud Security against Traditional Computing.	
3	**MODULE 3: Cloud Mechanisms**		
	1	Data Center Technology, Virtualization Technology, Web Technology,	15

		Multitenant Technology,	
	2	Scaling, Foundation of Cloud Scaling, Scaling Strategies in Cloud, Auto Scaling in Cloud, Cloud Bursting, Types of Scaling,	
	3	Capacity Planning, Capacity Planning at Different Service Levels,	
	4	Load Balancer, Two Levels of Balancing, Goals of Load Balancing, Categories of Load Balancing, Exploring Dynamic Load Balancing.	

4	**MODULE 4: Cloud Security Strategies**		
	1	Standards for Security: SAML OAuth, OpenID, SSL/TLS,	15
	2	Encrypting Data and Key Management,	
	3	Creating a Cloud Security Strategy,	
	4	The Future of Security in Cloud Computing.	

5	**Teacher Specific Module**	
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	15

Essential Readings:

1. Bhowmik, S., “Cloud computing”, Cambridge University Press, 2017.
2. Thomas, E., Zaigham, M., Ricardo, P “Cloud Computing Concepts, Technology & Architecture, Prentice Hall, 2013.

Suggested Readings:

1. Ronald L. Krutz, Russell Dean Vines, "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, 2010.
2. Tim Mather, SubraKumaraswamy, and ShahedLatif, ” Cloud Security and Privacy", O’Reilly Media, Inc., 2009

Assessment Rubrics:

Evaluation Type	Marks
End Semester Evaluation	**70**

Continuous Evaluation		**30**
a)	Test Paper- 1	5
b)	Model Exam	10
c)	Assignment(2 numbers)	10
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
Grand Total		**100**

KU6DSECSY304: AI-DRIVEN SOFTWARE ENGINEERING

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
6	DSE	300-399	**KU6DSECSY304**	4 (3T+1P)	75

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
3	2		35	65	100	1.5hrs.

Course Description:

The course provides experience on various processes used in Software industry for the development of a software product. The course enables to understand the evolution of Software Engineering and the role of Artificial Intelligence in transforming the SDLC.

Course Prerequisite: NIL

Course Outcomes:

CO No.	Expected Outcome	Learning Domains
1	Analyze limitations of traditional software engineering and explain AI integration across SDLC phases.	U, A
2	Apply machine learning techniques for software analytics including defect prediction, effort estimation, and fault localization.	A
3	Design and evaluate generative AI-based solutions for code generation, testing, documentation, and refactoring.	A,C
4	Develop AI-driven DevOps and agent-based automation strategies for intelligent software deployment and monitoring.	A, C

**Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)*

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	3			2			
CO 2	3		2				
CO 3	3	3	3	2			
CO 4	3	2	2	2		2	2

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	**UNIT**	**DESCRIPTION**	**HOURS**
1	**MODULE 1: Foundations of AI-Driven Software Engineering**		
	1	Evolution of Software Engineering (SE) and its Limitations - Introduction to AI in Software Engineering - AI integration across SDLC -	15
	2	Machine Learning for software analytics: Effort estimation -Defect prediction -Fault localization –	
	3	ML based Static and Dynamic code analysis - NLP for requirements engineering -	
	4	Intelligent Software architecture support - Search-based software engineering.	

2	**MODULE 2: Generative AI for Software Development**		
	1	Large Language Models for code generation - Prompt engineering for software tasks -	15
	2	Retrieval Augmented Generation (RAG) for software artifacts - AI-assisted documentation and specification generation -	
	3	Automated code review using LLMs -Test case generation using Generative AI - Programme synthesis and automated refactoring -	
	4	Evaluation metrics and benchmarking framework for generative code systems.	

3	**MODULE 3: DevOps, AIOps, Agentic AI and Autonomous Software Engineering**		
	1	**DevOps Foundations:** CI/CD pipelines - Infrastructure as Code – Monitoring and logging - AI-Driven DevOps (**AIOps**) -	15
	2	Log analysis and anomaly detection - Deployment failure prediction - Data-driven release decision support- Agile and Lean Practices in DevOps.	
	3	**Introduction to Agentic AI** - AI agents in SDLC phases-Tool augmented LLMs and function calling-multi-agent orchestration frameworks-	
	4	Autonomous CI/CD systems-Self-healing systems-Human-in-the-loop AI supervision.	

4	**MODULE 4: Secure and Responsible AI driven Software Engineering**		
	1	Security risks in AI generated code - Prompt injection and adversarial threats - Bias and reliability in AI-assisted development -	15
	2	Explainable AI for software systems - Responsible AI in SDLC-	
	3	Federated learning for secure software analytics- Evaluation frameworks for AI-driven SE systems-.	
	4	Research trends in AI in Software Engineering-Case Studies from Industry and Academia.	

5	**Teacher Specific Module**	
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	15

Essential Reading

1. Zhang, D., & Tsai, J. J. (Eds.). (2005). Machine learning applications in software engineering (Vol. 16). World Scientific.
2. Maria Virvou, George A. Tsihrintzis, Nikolaos G. Bourbakis, Lakhmi C. Jain. (Eds.). (2022), Handbook on Artificial Intelligence-Empowered Applied Software Engineering, VOL.1: Novel Methodologies to Engineering Smart Software Systems, Springer Cham

Suggested Readings:

1. Romero, J. R., Medina-Bulo, I., & Chicano, F. (Eds.). (2023). Optimising the software development process with artificial intelligence. Berlin: Springer.
2. Benala, T. R., Dehuri, S., Mall, R., & Favorskaya, M. N. (Eds.). (2025). Boosting Software Development Using Machine Learning. Springer.
3. Kadry, S., &Balasubramaniam, S. (Eds.). (2025). Generative AI for Software Development: Code Generation, Error Detection, Software Testing. Walter de Gruyter GmbH & Co KG.
4. Valentina Alto(2024), Building LLM Powered Applications, Packt Publishing Ltd.
5. Paul Iusztin, Maxime Labonne(2024), LLM Engineer's Handbook, Packt Publishing Ltd.
6. Chip Huyen(2024), AI Engineering: Building Applications with Foundation Models, O'Reilly Media
7. Humble, J., & Farley, D. (2018). The DevOps Handbook: How to Create World-Class Agility, Reliability, & Security in Technology Organizations. IT Revolution.

Assessment Rubrics:

Evaluation Type		**Marks**
End Semester Evaluation		**50 (Theory)** **15 (Practical)**
Continuous Evaluation		**35**
CE (Theory)		**25**
a)	Test Paper- 1	5
b)	Model Exam	10
c)	Assignment(2 numbers)	5
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
CE (Practical)		**10**
Total		**100**

KU6DSECSY305: AI FOR CYBER SECURITY

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
6	DSE	300-399	**KU6DSECSY305**	4 (3T+1P)	75

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
3	2		35	65	100	1.5hrs.

Course Description:

The course AI For Cyber Security equip students with a solid understanding of rule-based AI, machine learning, and deep learning techniques for addressing various cybersecurity challenges.

Course Prerequisite: NIL

Course Outcomes:

CO No.	Expected Outcome	Learning Domains
1	Analyze the effectiveness of rule-based AI and machine learning models in detecting cyber security threats and mitigating risks.	U, A
2	Distinguish between supervised and unsupervised learning approaches for phishing detection, intrusion detection, and anomaly analysis in cyber security.	A
3	Evaluate classification algorithms such as Bayesian models, SVMs, Decision Trees, and ensemble methods for malware detection and threat prediction.	A,C
4	Design deep learning models, including CNNs, RNNs, LSTMs, and GANs, for advanced applications like attack pattern generation and encrypted traffic analysis.	A, C

**Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)*

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	3			2			
CO 2	3		2				
CO 3	3	3	3	2			
CO 4	3	2	2	2		2	2

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	**UNIT**	**DESCRIPTION**	**HOURS**
1	**MODULE 1:**		
	1	Rule-Based AI vs. Machine Learning in Threat Detection, Neural Networks and Learning Algorithms for Cybersecurity Applications, Bias-Variance Tradeoffs in Cybersecurity Models,	15
	2	Reinforcement Learning for Adaptive Threat Mitigation, PCABased Feature Engineering for Anomaly Detection,	
	3	Supervised Learning in Phishing Detection, Unsupervised Learning for Intrusion Detection,	
	4	Automated Cyber Defense with Reinforcement Learning.	

2	**MODULE 2:**		
	1	Effectiveness of Bayesian, SVM, Decision Tree, and Random Forest classifiers in detecting cyber threats,	15
	2	, Performance of ensemble methods in improving malware detection accuracy,	
	3	Application of linear and logistic regression models for predicting security risks,	
	4	Use of supervised learning algorithms in phishing and APT detection.	

3	**MODULE 3:**		
	1	Partition-Based and Subspace Clustering for anomaly detection in network traffic,	15
	2	Incremental Clustering techniques for real-time cyber threat detection,	
	3	Spectral Clustering in identifying hidden attack patterns,	
	4	Hidden Markov Models for detecting rare cyber-attacks and advanced persistent threats.	

4	**MODULE 4:**		
	1	Deep neural networks for cyber threat classification, Deep Feed Forward Networks for malware detection,	15
	2	Convolutional Neural Networks for image-based phishing page detection,	
	3	Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) for time-series anomaly detection,	
	4	Generative Adversarial Networks (GANs) for generating attack patterns, Autoencoders for unsupervised anomaly detection in network traffic.	

5	**Teacher Specific Module**	
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	15

Essential Readings:

1. Tony Thomas, Athira P. Vijayaraghavan, Sabu Emmanuel, Machine Learning Approaches in Cybersecurity Analytics, Springer 2020.
2. Tony Thomas, RoopakSurendran, Teenu S John, MamounAlazab, Intelligent Mobile Malware Detection, CRC Press, Taylor and Francis, 2023.

3. Artificial Intelligence: A Modern Approach 4th Edition, Stuart Russell and Peter Norvig, Pearson, 2020.
4. Understanding Machine Learning: From Theory to Algorithms, ShaiShalevShwartz, ShaiBenDavid, Cambridge University Press, 2014.
5. Clarence Chio, David Freeman, Machine Learning & Security, O Reilly, 2018.
6. Deep Learning Applications for Cyber Security, Alazab, Mamoun, Tang, MingJian (Eds.), Springer, 2019.
7. Rakesh M. Verma, David J. Marchette, Cybersecurity Analytics, by Chapman and Hall/CRC, 2019.
8. Charu C. Aggarwal, Neural Networks and Deep Learning: A Textbook (Second Edition), Springer, 2023.

Suggested Readings:

1. Alexey Kleymenov, AmrThabet, Mastering Malware Analysis: The complete malware analyst's guide to combating malicious software, APT, cybercrime, and IoT attacks, 2019.
2. Monappa KA, Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware, Packt Publication, 2018.
3. Xin et al, Machine Learning and Deep Learning Methods for Cybersecurity, IEEE Access 2018.
4. Bowei Xi, Adversarial machine learning for cybersecurity and computer vision: Current developments and challenges, WIREs Computational Statistics, April 2020.
5. Mohammad Al-Rubaie, Privacy Preserving Machine Learning: Threats and Solutions, n IEEE Security and Privacy Magazine, 2018.
6. Aiyanyo et al, A Systematic Review of Defensive and Offensive Cybersecurity with Machine Learning, Applied Sciences, MDPI, Aug 2020.
7. Shaukat et al, A Survey on Machine Learning Techniques for Cyber Security in the Last Decade, IEEE Access, Dec 2020.
8. Anthony D. Joseph, Blaine Nelson, Benjamin I. P. Rubinstein, Adversarial Machine Learning, Cambridge University Press, 2019.

Assessment Rubrics:

Evaluation Type	**Marks**
End Semester Evaluation	**50 (Theory)** **15 (Practical)**
Continuous Evaluation	**35**
CE (Theory)	**25**

a)	Test Paper- 1	5
b)	Model Exam	10
c)	Assignment(2 numbers)	5
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
CE (Practical)		**10**
Total		**100**

KU6SECCSY302: IOT SECURITY

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
6	SEC	300-399	**KU6SECCSY302**	3	45

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
3	0	-	25	50	75	1.5 hrs

Course Description:

An IoT Security course teaches you how to identify, assess, and mitigate security risks across connected devices and networks. Students learn to detect vulnerabilities, secure hardware/firmware, and implement encryption to protect critical data and smart ecosystems from emerging cyber threats.

Course Prerequisite: NIL

Course Outcomes:

CO No.	Expected Outcome	Learning Domains
1	Incorporate the best practices learnt to identify the attacks and mitigate the same	U, A
2	Adopt the right security techniques and protocols during the design of IoT products	A
3	Describe the essential components of IoT	A,C
4	Find appropriate security/privacy solutions for IoT	A, C

****Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)***

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7

CO 1	3			2			
CO 2	3		2				
CO 3	3	3	3	2			
CO 4	3	2	2	2		2	2

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	**UNIT**	**DESCRIPTION**	**HOURS**
1	**MODULE 1:**		
	1	Fundamentals of IoT and Security and its need, Prevent Unauthorized Access to Sensor Data,	9
	2	Block ciphers, Introduction to Blockchain, Introduction of IoT devices, IoT Security Requirements,	
	3	M2M Security, Message integrity Modeling faults and adversaries Difference among IoT devices,	
	4	computers, and embedded devices.	
2	**MODULE 2:**		
	1	IoT and cyber-physical systems RFID Security, Authenticated encryption Byzantine Generals problem sensors and actuators in IoT,	9
	2	IoT security (vulnerabilities, attacks, and countermeasures),	
	3	Cyber Physical Object Security,	
	4	Hash functions Consensus algorithms and their scalability problems Accelerometer, photoresistor, buttons	
3	**MODULE 3:**		
	1	Security engineering for IoT development Hardware Security, Merkle trees and Elliptic curves digital signatures,	9
	2	verifiable random functions, Zero-knowledge systems motor, LED, vibrator,	
	3	IoT security lifecycle, Front-end System Privacy Protection,	

	4	Management, Secure IoT Databases, Public-key crypto (PKI), blockchain, the challenges, and solutions, analog signal vs. digital signal	

4	**MODULE 4:**		
	1	Data Privacy Networking Function Security Trees signature algorithms proof of work, Proof of stake,	9
	2	Networking in IoT Device/User Authentication in IoT IoT Networking Protocols,	
	3	Crypto-currencies,alternatives to Bitcoin consensus, Bitcoin scripting language and their use Real-time communication	
	4	Bitcoin P2P network, Ethereum and Smart Contracts,	

5	**Teacher Specific Module**	
	Directions	
	Teachers are expected to select relevant topics within the chosen subject area, giving special emphasis to advanced concepts and recent developments in the field. The content should be enriched with well-chosen case studies that highlight practical applications, contemporary issues, and emerging trends, thereby enabling students to gain both theoretical knowledge and contextual understanding.	9

Essential Readings:

1. B. Russell and D. Van Duren, “Practical Internet of Things Security,” Packt Publishing, 2016.
2. FeiHU,“Security and Privacy Internet of Things (IoTs):Models, Algorithms and Implementations”, CRC Press, 2016
3. Narayanan et al., “Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction,” Princeton University Press, 2016.

Suggested Readings:

1. A. Antonopoulos, “Mastering Bitcoin: Unlocking Digital Crypto currencies,” O’Reilly, 2014.
2. T. Alpcan and T. Basar, “Network Security: A Decision and Game-theoretic Approach,” Cambridge University Press, 2011.
3. Security and the IoT ecosystem, KPMG International, 2015.
4. Internet of Things: IoT Governance, Privacy and Security Issues” European Research Cluster.
5. Ollie Whitehouse, “Security of Things: An Implementers' Guide to Cyber-Security for Internet of Things Devices and Beyond”, NCC Group, 2014.

6. Josh Thompson, 'Blockchain: The Blockchain for Beginnings, Guide to Blockchain Technology and Blockchain Programming', Create Space Independent Publishing Platform, 2017.

Assessment Rubrics:

Evaluation Type		Marks
End Semester Evaluation		**50**
Continuous Evaluation		**25**
a)	Test Paper- 1	5
b)	Model exam	10
c)	Assignment	5
d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
Total		**75**