SAHYADRI
COLLEGE OF ENGINEERING & MANAGEMENT
An Autonomous Institution
MANGALURU

SOFTWARE ENGINEERING AND PROJECT MANAGEMENT

(Effective from the Academic Year 2023 - 2024)

VI SEMESTER

Course Code	**21CS61**		CIA Marks	50
Number of Contact Hours/Week (L:T:P:S)	3:0:0:0		SEE Marks	50
Total Contact Hours	40L		Exam Hours	03

CREDITS - 3

COURSE PREREQUISITES:

- Fundamentals of software Development activities, Management functions.

COURSE OBJECTIVES:

- Outline software engineering principles and activities involved in building large software programs.
- Identify ethical and professional issues and explain why they are of concern to Software Engineers.
- Describe the process of requirement gathering, requirement classification, requirement specification and requirements validation.
- Infer the fundamentals of object-oriented concepts, differentiate system models, use UML diagrams and apply design patterns.
- Explain the importance of Agile Software Development.
- Discuss various types of software testing practices and software evolution processes.
- Recognize the importance Project Management with its methods and methodologies.
- Identify software quality parameters and quantify software using measurements and metrics. List software quality standards and outline the practices involved

TEACHING - LEARNING STRATEGY:

Following are some sample strategies that can be incorporate for the Course Delivery

- Chalk and Talk Method/Blended Mode Method
- Power Point Presentation
- Expert Talk/Webinar/Seminar
- Video Streaming/Self-Study/Simulations
- Peer-to-Peer Activities
- Activity/Problem Based Learning
- Case Studies
- MOOC/NPTEL Courses
- Any other innovative initiatives with respect to the Course contents

COURSE CONTENTS

MODULE - I

Introduction: The evolving role of software, The changing nature of software, Software engineering, A Process Framework, Process Patterns, Process Assessment, Personal and Team Process Models, Process Technology, Product and Process. **Process Models**: Prescriptive models, Waterfall model, Incremental process models, Evolutionary process models, Specialized process models.	**8 Hours**

MODULE - II

Introduction, Modelling Concepts and Class Modelling: What is Object orientation? What is OO-development? OO Themes; Evidence for usefulness of OO development; OO modelling history. Modelling as Design technique: Modelling, abstraction, The Three models. Class Modelling: Object and Class Concept, Link and associations concepts, Generalization and Inheritance, A sample class model, Navigation of class models, and UML diagrams	**8 Hours**

MODULE - III	
Software Testing: A Strategic Approach to Software Testing, Strategic Issues, Test Strategies for Conventional Software, Test Strategies for Object -Oriented Software, Validation Testing, System Testing, The Art of Debugging. Agile Methodology: Before Agile – Waterfall, Agile Development.	**8 Hours**
MODULE - IV	
Introduction to Project Management: Introduction, Project and Importance of Project Management, Contract Management, Activities Covered by Software Project Management, Plans, Methods and Methodologies, some ways of categorizing Software Projects, Stakeholders, Setting Objectives, Business Case, Project Success and Failure, Management and Management Control, Project Management life cycle, Traditional versus Modern Project Management Practices.	**8 Hours**
MODULE - V	
Activity Planning: Objectives of Activity Planning, When to Plan, Project Schedules, Sequencing and Scheduling Activities, Network Planning Models, Forward Pass– Backward Pass, identifying critical path, Activity Float, Shortening Project Duration, Activity on Arrow Networks. Software Quality: Introduction, the place of software quality in project planning, Importance of software quality, software quality models, ISO 9126, quality management systems, process capability models, techniques to enhance software quality, quality plans.	**8 Hours**

COURSE OUTCOMES

Upon completion of this course, the students will be able to:

CO No.	Course Outcome Description	Bloom's Taxonomy Level
CO1	Understand the activities involved in software engineering and analyse the role of various process models	CL2
CO2	Explain the basics of object-oriented concepts and build a suitable class model using modelling techniques	CL2
CO3	Interpret various software testing methods and to understand the importance of agile methodology.	CL2
CO4	Apply the Concepts of project planning and quality management in software development	CL3
CO5	Illustrate the importance of activity planning and its models	CL2

CO-PO-PSO MAPPING

CO No.	Programme Outcomes (PO)												Programme Specific Outcome (PSO)		
	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3
CO1	2	1				1		2	1	1		2	1	1	
CO2	2	2	2		2	1		2	2	2	2	2	2	1	
CO3	2	2	2		2			2	2	3	1	2	3	1	1
CO4	2	2	2		2			2	3	3	2	2	3	1	1
CO5	2	2	2		2	2	2	2	3	3	2	2	3	1	1

3: Substantial (High)	2: Moderate (Medium)	1: Poor (Low)

ASSESSMENT STRATEGY

Assessment will be both CIA and SEE. Student's learning will be assessed using Direct and Indirect methods.

Sl. No.	Assessment Description	Weightage (%)	Max. Marks
1	**Continuous Internal Assessment (CIA)**	**100 %**	**50**
	Continuous Internal Evaluation (CIE)	60 %	30
	Assignments	40 %	20
2	**Semester End Examination (SEE)**	**100 %**	**50**

ASSESSMENT DETAILS

Continuous Internal Assessment (CIA) (50%)				
Continuous Internal Evaluation (CIE) (60%)			**Assignment/Activities (40%)**	**Semester End Exam (SEE) (50%)**
I	**II**	**III**		
Syllabus Coverage			**Syllabus Coverage**	**Syllabus Coverage**
30%	**30%**	**40%**	**100%**	**100%**
M I			M I	M I
M II	M II		M II	M II
	M III		M III	M III
		M IV	M IV	M IV
		M V	M V	M V

Note: For Examinations (both CIE and SEE), the question papers shall contain the questions mapped to the appropriate Bloom's Level. Any COs mapped with higher cognitive Bloom's Level may also be assessed through the assignments.

ASSIGNMENT TYPES WITH WEIGHTAGES

Sl. No.	Assignment Description	Max. Weightage (%)	Max. Marks
1	Written Assignments	25 %	05
2	Quiz	10 %	02
3	Case Studies	25 %	05
4	Seminar/Presentation	15 %	03
5	Peer-to-Peer Learning	10 %	02
6	Activity Based Learning	50 %	10
7	Project Based Learning	50 %	10
8	Field Work + Report	50 %	10
9	Industry Visit + Report	50 %	10
10	NPTEL/MOOC Courses – Registration and Assignment Submissions	50 %	10
	NPTEL Certification	75 %	15
11	Any other Innovative Assignments (CL4 and above)	50 %	10

Note: The assignments mentioned above may be provided appropriately to the students belonging to different bands.

SEE QUESTION PAPER PATTERN:

- The question paper will have **TEN** full questions from **FIVE** Modules.
- There will be 2 full questions from each module. Every question will carry a maximum of 20 marks.
- Each full question may have a maximum of four sub-questions covering all the topics under a module.
- The students will have to answer FIVE full questions, selecting one full question from each module.

TEXT BOOKS:

1. Roger S. Pressman: Software Engineering-A Practitioners approach, 6th Edition, Tata McGraw Hill.
2. Michael Blaha, James Rumbaugh: Object Oriented Modelling and Design with UML, 2nd Edition, Pearson Education, 2005.
3. Bob Hughes, Mike Cotterell, Rajib Mall: Software Project Management, 6th Edition, McGraw Hill Education, 2018.
4. Deepak Gaikwad, Viral Thakkar, DevOps Tools From Practitioner's Viewpoint, Wiley.

REFERENCE WEB LINKS AND VIDEO LECTURES (E-RESOURCES):

1. **https://onlinecourses.nptel.ac.in/noc20_cs68/preview**
2. **https://www.youtube.com/watch?v=WxkP5KR_Emk&list=PLrjkTql3jnm9b5nrggx7Pt1G4UAHeFl**
3. **http://elearning.vtu.ac.in/econtent/CSE.php**
4. **http://elearning.vtu.ac.in/econtent/courses/video/CSE/15CS42.html**
5. **https://nptel.ac.in/courses/128/106/128106012/ (DevOps)**

CRYPTOGRAPHY AND NETWORK SECURITY

(Effective from the Academic Year 2023 - 2024)

VI SEMESTER

Course Code	**21CY62**	CIA Marks	50
Number of Contact Hours/Week (L: T: P: S)	3:0:2:0	SEE Marks	50
Total Hours of Pedagogy	40L + 20P	Exam Hours	03

CREDITS – 4

COURSE PREREQUISITES:

- Fundamental knowledge of Mathematics and Computer Networks.

COURSE OBJECTIVES:

- Define cryptography and its principles
- Explain Cryptography algorithms
- Illustrate Public and Private key cryptography
- Explain Key management, distribution and certification

TEACHING - LEARNING STRATEGY:

Following are some sample strategies that can be incorporate for the Course Delivery

- Chalk and Talk Method/Blended Mode Method
- Power Point Presentation
- Expert Talk/Webinar/Seminar
- Video Streaming/Self-Study/Simulations
- Peer-to-Peer Activities
- Activity/Problem Based Learning
- Case Studies
- MOOC/NPTEL Courses
- Any other innovative initiatives with respect to the Course contents

COURSE CONTENTS

MODULE - I

8 Hours

Classical Encryption Techniques
Symmetric Cipher Model, Cryptography, Cryptanalysis and Brute-Force Attack, Substitution Techniques, Caesar Cipher, Monoalphabetic Cipher, Playfair Cipher, Hill Cipher, Polyalphabetic Cipher, One Time Pad.
Block Ciphers and the data encryption standard:
Traditional block Cipher structure, stream Ciphers and block Ciphers, Motivation for the Feistel Cipher structure, the Feistel Cipher, The data encryption standard: DES encryption, DES decryption, A DES example: results, the avalanche effect, the strength of DES: the use of 56-Bit Keys, the nature of the DES algorithm, timing attacks, Block cipher design Principles: number of rounds, design of function F, key schedule algorithm

MODULE - II

8 Hours

Advanced Encryption Standard: AES Structure, AES Transformation
Public-Key Cryptography and RSA:
Principles of public-key cryptosystems. Public-key cryptosystems. Applications for public-key cryptosystems, requirements for public-key cryptosystems. public-key cryptanalysis. The RSA algorithm, description of the algorithm, computational aspects, the security of RSA.
Other Public-Key Cryptosystems:
Diffie-hellman key exchange, The algorithm, key exchange protocols, man in the middle attack, Elgamal Cryptographic systems

MODULE - III	
Elliptic curve arithmetic, abelian groups, elliptic curves over real numbers, elliptic curves over Zp, elliptic curves over GF(2m), Elliptic curve cryptography, Analog of Diffie-hellman key exchange, Elliptic curve encryption/ decryption, security of Elliptic curve cryptography, Pseudorandom number generation based on an asymmetric cipher, PRNG based on RSA. **Key Management and Distribution**: Symmetric key distribution using Symmetric encryption, A key distribution scenario, Hierarchical key control, session key lifetime, a transparent key control scheme, Decentralized key control, controlling key usage, Symmetric key distribution using asymmetric encryption, simple secret key distribution, secret key distribution with confidentiality and authentication, A hybrid scheme, distribution of public keys, public announcement of public keys, publicly available directory, public key authority, public keys certificates.	**8 Hours**
MODULE - IV	
X-509 certificates. Certificates, X-509 version 3, public key infrastructure. **User Authentication:** Remote user Authentication principles, Mutual Authentication, one way Authentication, remote user Authentication using Symmetric encryption, Mutual Authentication, one way Authentication, Kerberos, Motivation, Kerberos version 4, Kerberos version 5, Remote user Authentication using Asymmetric encryption, Mutual Authentication, one way Authentication. **Electronic Mail Security:** Pretty good privacy, notation, operational; description, S/MIME, RFC5322, Multipurpose internet mail extensions, S/MIME functionality, S/MIME messages, S/MIME certificate processing, enhanced security services, Domain keys identified mail, internet mail architecture, E-Mail threats, DKIM strategy, DKIM functional flow.	**8 Hours**
MODULE - V	
IP Security: IP Security overview, applications of IPsec, benefits of IPsec, Routing applications, IPsec documents, IPsec services, transport and tunnel modes, IP Security policy, Security associations, Security associations database, Security policy database, IP traffic processing, Encapsulating Security payload, ESP format, encryption and authentication algorithms, Padding, Anti replay service Transport and tunnel modes, combining security associations, authentication plus confidentiality, basic combinations of security associations, internet key exchange, key determinations protocol, header and payload formats, cryptographic suits.	**8 Hours**

COURSE OUTCOMES

Upon completion of this course, the students will be able to:

CO No.	Course Outcome Description	Bloom's Taxonomy Level
CO1	Discuss the classical encryption techniques and block ciphers and the data encryption standard	CL3
CO2	Describe the public key cryptography and RSA and the other Public Key Cryptosystems	CL3
CO3	Solve the Elliptic curve arithmetic, abelian groups, elliptic curves over real numbers, Illustrate the need of the key management and distribution	CL3
CO4	Describe the User Authentication, Electronic Mail Security	CL3
CO5	Illustrate the IP security, transport and tunnel modes	CL2

LABORATORY COMPONENTS			
Exp. No.	**Experiment Description**	**CO No.**	**Bloom's Taxonomy Level**
1.	Demonstrate the Mono-alphabetic Substitution Cipher using java program. And demonstrate breaking cipher using virtual lab.	CO1	CL3
2.	Demonstrate the. Data Encryption Standard (DES) using java programing	CO1	CL3
3.	Demonstrate the Symmetric Key Encryption Standards (AES) .	CO2	CL3
4.	Demonstrate Diffie-Hellman Key Establishment.	CO2	CL3
5.	Demonstrate Digital Signature using RSA Algorithm .	CO3	CL3
6.	Demonstrate Kerberos Authentication, simulate some of the key steps in a Kerberos system.	CO4	CL3
7.	Demonstrate IP Security using Cisco packet tracer experimental setup.	CO5	CL3
Above programs can be explored with suitably using java libraries or python libraries and simulation can be performed with virtual lab.			

CO-PO-PSO MAPPING

CO No.	**Programme Outcomes (PO)**												**Programme Specific Outcome (PSO)**		
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**	**3**
CO1	3	3	3							1		1	2	1	
CO2	3	3	3							1		1	2	1	
CO3	3	3	3	1	2				1	1		1	2	1	
CO4	3	3	3	1	2				1	1		1	2	1	
CO5	3	3	3							1		1	2	1	
3: Substantial (High)					**2: Moderate (Medium)**					**1: Poor (Low)**					

ASSESSMENT STRATEGY

Assessment will be both CIA and SEE. Students learning will be assessed using Direct and Indirect methods:

Sl. No.	**Assessment Description**	**Weightage (%)**	**Max. Marks**
1	**Continuous Internal Assessment (CIA)**	**100 %**	**50**
	Continuous Internal Evaluation (CIE)	60 %	30
	Practical Session (Laboratory Component)	40 %	20
2	**Semester End Examination (SEE)**	**100 %**	**50**

ASSESSMENT DETAILS

Continuous Internal Assessment (CIA) (50%)				
Continuous Internal Evaluation (CIE) (60%)			**Practical Sessions (40%)**	**Semester End Exam (SEE) (50%)**
I	**II**	**III**		
Syllabus Coverage			**Syllabus Coverage**	**Syllabus Coverage**
40%	**30%**	**30%**	**100%**	**100%**
MI			MI	MI
MII	MII		MII	MII
	MIII		MIII	MIII
		MIV	MIV	MIV

		MV	MV	MV

NOTE:

- Assessment will be both CIA and SEE.
- The practical sessions of the IPCC shall be for CIE only.
- The Theory component of the IPCC shall be for both CIA and SEE respectively.
- The questions from the practical sessions shall be included in Theory SEE.

Note: For Examinations (both CIE and SEE), the question papers shall contain the questions mapped to the appropriate Bloom's Level. Any COs mapped with higher cognitive Bloom's Level may also be assessed through the assignments.

SEE QUESTION PAPER PATTERN:

1. The question paper will have **TEN** full questions from **FIVE** Modules
2. There will be 2 full questions from each module. Every question will carry a maximum of 20 marks.
3. Each full question may have a maximum of four sub-questions covering all the topics under a module.
4. The students will have to answer FIVE full questions, selecting one full question from each module.

TEXT BOOKS:

1. William Stallings: Cryptography and Network Security, Pearson 6th edition.
2. V K Pachghare: Cryptography and Information Security, PHI 2nd Edition

CYBER SECURITY FUNDAMENTALS AND LAWS

(Effective from the Academic Year 2023 - 2024)

VI SEMESTER

Course Code	**21CY63**	CIA Marks	50
Number of Contact Hours/Week (L: T: P: S)	3:0:0:0	SEE Marks	50
Total Hours of Pedagogy	**40L**	Exam Hours	03

CREDITS – 3

COURSE PREREQUISITES:

- Fundamental knowledge of Cyber Security.

COURSE OBJECTIVES:

- Understand basic concepts of Cyber Crimes.
- Ability to identify the attacks in Cyber Crimes
- Able to specify the suitable methods used in Cyber Crime
- Ability to face cyber security challenges
- Understand Cyber Security

TEACHING - LEARNING STRATEGY:

Following are some sample strategies that can be incorporate for the Course Delivery

- Chalk and Talk Method/Blended Mode Method
- Power Point Presentation
- Expert Talk/Webinar/Seminar
- Video Streaming/Self-Study/Simulations
- Peer-to-Peer Activities
- Activity/Problem Based Learning
- Case Studies
- MOOC/NPTEL Courses
- Any other innovative initiatives with respect to the Course contents

COURSE CONTENTS

MODULE - I	
Cyber Crime: Cybercrime and information security, Classification of cybercrimes, cybercrime legal perspective and Indian Perspective. Cybercrime and Indian ITA 2000, a global perspective on cybercrime, cybercrime ERA	**8 Hours**
MODULE – II	
Cyber Offenses: How Criminals plan the Attacks, Social Engineering, Cyber stalking, Cyber Cafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Attack Vector, Cloud Computing.	**8 Hours**
MODULE - III	
Cybercrime: Mobile and Wireless Devices: Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for Organizations, Organizational Measures for Handling Mobile, Organizational Security Policies an Measures in Mobile Computing Era, Laptop	**8 Hours**
MODULE - IV	
Types of Attacks and Cybercrime: Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Keyloggers and Spywares, Virus and Worms, Trojan Horse and Backdoors, Steganography, DoS and DDoS attacks, SQL Injection, Buffer Overflow	**8 Hours**
MODULE – V	
Cyber Security Organizational Policies, Risk and Challenges: Organizational Implications. Introduction, Cost of Cybercrimes and IPR issues, Web threats for Organizations, Security and Privacy Implications, Social media marketing: Security Risks and Perils for Organizations, Social Computing and the associated challenges for Organizations, FAQs on the Digital Personal Data Protection Act, 2023 (DPDP Act)	**8 Hours**

COURSE OUTCOMES

Upon completion of this course, the students will be able to:

CO No.	Course Outcome Description	Bloom's Taxonomy Level
CO1	Comprehensive understanding of fundamental cyber security concepts, threats, vulnerabilities, and the measures necessary to protect information systems and assets	CL2
CO2	Comprehending the attack vectors utilized by cybercriminals and the challenges presented by cloud computing in the domain of cybercrime	CL2
CO3	The ability to perceive the unique challenges and security implications associated with the widespread use of mobile and wireless devices.	CL2
CO4	Understanding of various cyberattacks, the tools and techniques used by cybercriminals, and the countermeasures to mitigate and prevent these threats.	CL2
CO5	A thorough insight into the ramifications of cyber security for organizations.	CL2

CO-PO-PSO MAPPING

CO No.	Programme Outcomes (PO)												Programme Specific Outcome (PSO)		
	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3
CO1	3	1	1	1	3				3			3	3	3	3
CO2	3	1	1	1	3				3			3	3	3	3
CO3	3	2	2	1	3				3			3	3	3	3
CO4	3	2	2	1	3				3			3	3	3	3
CO5	3	3	2	1	3				3			3	3	3	3

3: Substantial (High)	2: Moderate (Medium)	1: Poor (Low)

ASSESSMENT STRATEGY

Assessment will be both CIA and SEE. Students learning will be assessed using Direct and Indirect methods:

Sl. No.	Assessment Description	Weightage (%)	Max. Marks
1	**Continuous Internal Assessment (CIA)**	**100 %**	**50**
	Continuous Internal Evaluation (CIE)	60 %	30
	Assignments	40 %	20
2	**Semester End Examination (SEE)**	**100 %**	**50**

ASSESSMENT DETAILS

Continuous Internal Assessment (CIA) (50%)				Semester End Exam (SEE) (50%)
Continuous Internal Evaluation (CIE) (60%)			Assignment/ Activities (40%)	
I	II	III		
Syllabus Coverage			Syllabus Coverage	Syllabus Coverage
40%	30%	30%	100%	100%
MI			MI	MI
MII	MII		MII	MII
	MIII		MIII	MIII
		MIV	MIV	MIV
		MV	MV	MV

Note: For Examinations (both CIE and SEE), the question papers shall contain the questions mapped to the appropriate Bloom's Level. Any COs mapped with higher cognitive Bloom's Level may also be assessed through the assignments.

ASSIGNMENT TYPES WITH WEIGHTAGES

Sl. No.	Assignment Description	Max. Weightage (%)	Max. Marks
1	Written Assignments	25 %	05
2	Quiz	10 %	02
3	Case Studies	25 %	05
4	Seminar/Presentation	15 %	03
5	Peer - to - Peer Learning	10 %	02
6	Activity Based Learning	50 %	10
7	Project Based Learning	50 %	10
8	Field Work + Report	50 %	10
9	Industry Visit + Report	50 %	10
10	NPTEL/MOOC Courses – Registration and Assignment Submissions	50 %	10
	NPTEL Certification	75 %	15
11	Any other Innovative Assignments (CL4 and above)	50 %	10

Note: The assignments mentioned above may be provided appropriately to the students belonging to different bands

SEE QUESTION PAPER PATTERN:

- The question paper will have **TEN** full questions from **FIVE** Modules
- There will be 2 full questions from each module. Every question will carry a maximum of 20 marks.
- Each full question may have a maximum of four sub-questions covering all the topics under a module.
- The students will have to answer FIVE full questions, selecting one full question from each module.

TEXT BOOKS:

1. "Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd.
2. Digital Personal Data Protection Act, 2023: A Bare Act by Taxmann's Publications
3. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRC Press.
4. Introduction to Cyber Security, Chwan-Hwa(john) Wu, J. David Irwin. CRC Press T&F Group

SAHYADRI
COLLEGE OF ENGINEERING & MANAGEMENT
An Autonomous Institution
MANGALURU

SECURE CODING

(Effective from the Academic Year 2023 - 2024)

VI SEMESTER

Course Code	**21CY641**	CIA Marks	50
Number of Contact Hours/Week (L: T: P: S)	3:0:0:0	SEE Marks	50
Total Hours of Pedagogy	**40L**	Exam Hours	03

CREDITS – 3

COURSE PREREQUISITES:

- Programming Experience: A strong foundation in programming using languages like Java, Python, or C/C++ is essential.
- Basic System Security Concepts

COURSE OBJECTIVES:

- Understand Security Threats: Develop an awareness of common security threats and vulnerabilities in software development, enabling students to identify potential risks and their impact on applications.

TEACHING - LEARNING STRATEGY:

Following are some sample strategies that can be incorporate for the Course Delivery

- Chalk and Talk Method/Blended Mode Method
- Power Point Presentation
- Expert Talk/Webinar/Seminar
- Video Streaming/Self-Study/Simulations
- Peer-to-Peer Activities
- Activity/Problem Based Learning
- Case Studies
- MOOC/NPTEL Courses
- Any other innovative initiatives with respect to the Course contents

COURSE CONTENTS

MODULE - I	
Running with Scissors: Gauging the threat, Security concepts. **Strings:** Common String Manipulation errors - Improperly Bounded String Copies - Off-by-One Errors - Null Termination Errors - String Truncation - String Errors without Functions, String vulnerabilities - Buffer Overflow - Process memory organization – Stack management – Stack smashing, Mitigation techniques – String handling functions.	**8 Hours**
MODULE - II	
Dynamic Memory Management – C Memory management functions, Common C Memory Management Errors – Initialization Errors - Failing to Check Return Values – Dereferencing Null or Invalid Pointers - Referencing Freed Memory - Freeing Memory Multiple Times - Memory Leaks - Zero-Length Allocations, Memory Managers, Doug Lea's Memory Allocator	**8 Hours**
MODULE - III	
Integer Security: Introduction to integer types, Integer Data Types, Integer Conversions, Integer operations, Integer Vulnerabilities, Mitigation strategies- Integer type selection- Abstract Data types - Range checking - secure Integer libraries.	**8 Hours**
MODULE – IV	
Formatted Output: Variadic Functions, Formatted Output Functions, Stack Randomization, Mitigation Strategies.	**8 Hours**
MODULE - V	
Concurrency: Multithreading, Parallelism, Performance Goals, Common Errors, Mitigation Strategies, Mitigation pitfalls. **File I/O**: TOCTOU, Mitigation strategies.	**8 Hours**

COURSE OUTCOMES

Upon completion of this course, the students will be able to:

CO No.	Course Outcome Description	Bloom's Taxonomy Level
CO1	Understand the common security threats in software applications and identify/mitigate vulnerabilities stemming from string manipulation errors.	CL2
CO2	Identify and mitigate the vulnerabilities based on dynamic memory management errors	CL2
CO3	Apply strategies to identify and address vulnerabilities associated with integer operations.	CL3
CO4	Identify and mitigate the vulnerabilities due to errors in formatted output functions	CL3
CO5	Demonstrate the ability to identify and effectively mitigate vulnerabilities resulting from errors in both concurrency and file I/O operations.	CL3

CO-PO-PSO MAPPING

CO No.	Programme Outcomes (PO)												Programme Specific Outcome (PSO)		
	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3
CO1	3	3	2		2				2			2	3	2	
CO2	3	3	2		2				2			2	3	2	
CO3	3	3	2		2				2			2	3	2	
CO4	3	3	2		2				2			2	3	2	
CO5	3	3	2		2				2			2	3	2	

3: Substantial (High)	2: Moderate (Medium)	1: Poor (Low)

ASSESSMENT STRATEGY

Assessment will be both CIA and SEE. Students learning will be assessed using Direct and Indirect methods:

Sl. No.	Assessment Description	Weightage (%)	Max. Marks
1	**Continuous Internal Assessment (CIA)**	**100 %**	**50**
	Continuous Internal Evaluation (CIE)	60 %	30
	Assignments	40 %	20
2	**Semester End Examination (SEE)**	**100 %**	**50**

ASSESSMENT DETAILS

Continuous Internal Assessment (CIA) (50%)				
Continuous Internal Evaluation (CIE) (60%)			Assignment/ Activities (40%)	Semester End Exam (SEE) (50%)
I	II	III		
Syllabus Coverage			Syllabus Coverage	Syllabus Coverage
40%	30%	30%	100%	100%
MI			MI	MI
MII	MII		MII	MII
	MIII		MIII	MIII
		MIV	MIV	MIV
		MV	MV	MV

Note: For Examinations (both CIE and SEE), the question papers shall contain the questions mapped to the appropriate Bloom's Level. Any COs mapped with higher cognitive Bloom's Level may also be assessed through the assignments.

ASSIGNMENT TYPES WITH WEIGHTAGES			
Sl. No.	**Assignment Description**	**Max. Weightage (%)**	**Max. Marks**
1	Written Assignments	25 %	05
2	Quiz	10 %	02
3	Case Studies	25 %	05
4	Seminar/Presentation	15 %	03
5	Peer - to - Peer Learning	10 %	02
6	Activity Based Learning	50 %	10
7	Project Based Learning	50 %	10
8	Field Work + Report	50 %	10
9	Industry Visit + Report	50 %	10
10	NPTEL/MOOC Courses – Registration and Assignment Submissions	50 %	10
	NPTEL Certification	75 %	15
11	Any other Innovative Assignments (CL4 and above)	50 %	10

Note: The assignments mentioned above may be provided appropriately to the students belonging to different bands

SEE QUESTION PAPER PATTERN:

- The question paper will have **TEN** full questions from **FIVE** Modules
- There will be 2 full questions from each module. Every question will carry a maximum of 20 marks.
- Each full question may have a maximum of four sub-questions covering all the topics under a module.
- The students will have to answer FIVE full questions, selecting one full question from each module.

TEXT BOOKS:

1. Textbook 1: "Secure Coding in C and C++" by Robert C. Seacord
2. OWASP Testing Guide" by The OWASP Foundation
3. Secure Programming with Static Analysis, by Brian Chess and Jacob West
4. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" by Dafydd Stuttard and Marcus Pinto

REFERENCE WEB LINKS AND VIDEO LECTURES (E - RESOURCES):

1. https://owasp.org/
2. https://developer.mozilla.org/en-US/docs/Web/Security
3. https://developers.google.com/web/fundamentals/security
4. https://www.youtube.com/playlist?list=PLNYkxOF6rcIDjlCx1Pcph7R_0Bux853mJ
5. https://www.pluralsight.com/courses/secure-coding-best-practices

WEB APLLICATION SECURITY

(Effective from the Academic Year 2023 - 2024)

VI SEMESTER

Course Code	**21CY642**	CIA Marks	50
Number of Contact Hours/Week (L: T: P: S)	3:0:0:0	SEE Marks	50
Total Hours of Pedagogy	**40L**	Exam Hours	03

CREDITS – 3

COURSE PREREQUISITES:

- User interface, a backend infrastructure, a database, and security features.

COURSE OBJECTIVES:

- To reveal the underlying in web application.
- To identify and aid in fixing any security vulnerabilities during the web development process.
- To understand the security principles in developing a reliable web application.

TEACHING - LEARNING STRATEGY:

Following are some sample strategies that can be incorporate for the Course Delivery

- Chalk and Talk Method/Blended Mode Method
- Power Point Presentation
- Expert Talk/Webinar/Seminar
- Video Streaming/Self-Study/Simulations
- Peer-to-Peer Activities
- Activity/Problem Based Learning
- Case Studies
- MOOC/NPTEL Courses
- Any other innovative initiatives with respect to the Course contents

COURSE CONTENTS

MODULE - I

Web Application (In)Security: The Evolution of Web Applications, Common Web Application Functions, Benefits of Web Applications, Web Application Security. **Core Defense Mechanisms:** Handling User Access Authentication, Session Management, Access Control, Handling User Input, Varieties of Input Approaches to Input Handling, Boundary Validation. Multistep Validation and Canonicalization, Handling Attackers, Handling Errors, Maintaining Audit Logs, Alerting Administrators, Reacting to Attacks.	**8 Hours**

MODULE - II

Web Application Technologies: The HTTP Protocol, HTTP Requests, HTTP Responses, HTTP Methods, URLs, REST, HTTP Headers, Cookies, Status Codes, HTTPS, HTTP Proxies, HTTP Authentication, Web Functionality, Server-Side Functionality, Client-Side Functionality, State and Sessions, Encoding Schemes, URL Encoding, Unicode Encoding, HTML Encoding, Base64 Encoding, Hex Encoding, Remoting and Serialization Frameworks.	**8 Hours**

MODULE - III

Mapping the Application: Enumerating Content and Functionality, Web Spidering, User Directed Spidering, Discovering Hidden Content, Application Pages Versus Functional Paths, Discovering Hidden Parameters, Analyzing the Application, Identifying Entry Points for User Input, Identifying Server-Side Technologies, Identifying Server-Side Functionality, Mapping the Attack Surface.	**8 Hours**

MODULE - IV

Attacking Authentication: Authentication Technologies, Design Flaws in Authentication Mechanisms, Bad Passwords, Brute-Forcible Login, Verbose Failure Messages, Vulnerable Transmission of Credentials, Password Change, Functionality, Forgotten Password Functionality, “Remember Me” Functionality, User	**8 Hours**

Impersonation, Functionality Incomplete, Validation of Credentials, Nonunique Usernames, Predictable Usernames, Predictable Initial Passwords, Insecure Distribution of Credentials. **Attacking Access Controls:** Common Vulnerabilities, Completely Unprotected, Functionality Identifier-Based Functions, Multistage Functions, Static Files, Platform Misconfiguration, Insecure Access Control Methods.	

MODULE - V

Attacking Data Stores: Injecting into Interpreted Contexts, Bypassing a Login, Injecting into SQL, Exploiting a Basic Vulnerability Injecting into Different Statement Types, Finding SQL Injection Bugs, Fingerprinting the Database, The UNION Operator, Extracting Useful Data, Extracting Data with UNION, Bypassing Filters, Second-Order SQL Injection, Advanced Exploitation Beyond SQL Injection: Escalating the Database Attack, Using SQL Exploitation Tools, SQL Syntax and Error Reference, Preventing SQL.	**8 Hours**

COURSE OUTCOMES

Upon completion of this course, the students will be able to:

CO No.	Course Outcome Description	Bloom's Taxonomy Level
CO1	Understand Knowledge of web application's vulnerability and malicious attacks.	CL2
CO2	Understand the basic web technologies used for web application development.	CL2
CO3	Understands the basic concepts of Mapping the application.	CL2
CO4	Demonstrate different attacking illustrations.	CL2
CO5	Understanding Basic concepts of Attacking Data Stores.	CL2

CO-PO-PSO MAPPING

CO No.	Programme Outcomes (PO)												Programme Specific Outcome (PSO)		
	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3
CO1	2	2				2							2	2	2
CO2	2	2	2			2							2	2	2
CO3	2	2	2			2							2	2	2
CO4		2	2			2							2	2	2
CO5	2	2				2							2	2	2
3: Substantial (High)					2: Moderate (Medium)					1: Poor (Low)					

ASSESSMENT STRATEGY

Assessment will be both CIA and SEE. Students learning will be assessed using Direct and Indirect methods:

Sl. No.	Assessment Description	Weightage (%)	Max. Marks
1	**Continuous Internal Assessment (CIA)**	**100 %**	**50**
	Continuous Internal Evaluation (CIE)	60 %	30
	Assignments	40 %	20
2	**Semester End Examination (SEE)**	**100 %**	**50**

ASSESSMENT DETAILS

Continuous Internal Assessment (CIA) (50%)				Semester End Exam (SEE) (50%)
Continuous Internal Evaluation (CIE) (60%)			Assignment/ Activities (40%)	
I	II	III		
Syllabus Coverage			Syllabus Coverage	Syllabus Coverage
40%	30%	30%	100%	100%
MI			MI	MI
MII	MII		MII	MII
	MIII		MIII	MIII
		MIV	MIV	MIV
		MV	MV	MV

Note: For Examinations (both CIE and SEE), the question papers shall contain the questions mapped to the appropriate Bloom's Level. Any COs mapped with higher cognitive Bloom's Level may also be assessed through the assignments.

ASSIGNMENT TYPES WITH WEIGHTAGES

Sl. No.	Assignment Description	Max. Weightage (%)	Max. Marks
1	Written Assignments	25 %	05
2	Quiz	10 %	02
3	Case Studies	25 %	05
4	Seminar/Presentation	15 %	03
5	Peer - to - Peer Learning	10 %	02
6	Activity Based Learning	50 %	10
7	Project Based Learning	50 %	10
8	Field Work + Report	50 %	10
9	Industry Visit + Report	50 %	10
10	NPTEL/MOOC Courses – Registration and Assignment Submissions	50 %	10
	NPTEL Certification	75 %	15
11	Any other Innovative Assignments (CL4 and above)	50 %	10

Note: The assignments mentioned above may be provided appropriately to the students belonging to different bands

SEE QUESTION PAPER PATTERN:

- The question paper will have **TEN** full questions from **FIVE** Modules
- There will be 2 full questions from each module. Every question will carry a maximum of 20 marks.
- Each full question may have a maximum of four sub-questions covering all the topics under a module.
- The students will have to answer FIVE full questions, selecting one full question from each module.

TEXT BOOKS:

1. Defydd Stuttard, Marcus Pinto Wiley Publishing, Second Edition.
2. Professional Pen Testing for Web application, Andres Andreu, Wrox Press.
3. Carlos Serrao, Vicente Aguilera, Fabio Cerullo, "Web Application Security" Springer; 1st Edition
4. Joel Scambray, Vincent Liu, Caleb Sima, "Hacking exposed", McGraw-Hill; 3rd Edition, (October, 2010).
5. OReilly Web Security Privacy and Commerce 2nd Edition 2011.
6. Software Security Theory Programming and Practice, Richard sinn, Cengage Learning.
7. Database Security and Auditing, Hassan, Cengage Learning.

SAHYADRI
COLLEGE OF ENGINEERING & MANAGEMENT
An Autonomous Institution
MANGALURU

SOCIAL NETWORK ANALYSIS

(Effective from the Academic Year 2023 - 2024)

VI SEMESTER

Course Code	**21CS643**	CIA Marks	50
Number of Contact Hours/Week (L: T: P: S)	3:0:0:0	SEE Marks	50
Total Hours of Pedagogy	**40L**	Exam Hours	03

CREDITS – 3

COURSE PREREQUISITES:

- Fundamental knowledge of Mathematics, Data Structures and algorithms.

COURSE OBJECTIVES:

- To understand the science of networks, including the principles of graph theory and key statistical properties of network.
- To acquire a working knowledge of descriptive network analysis techniques.
- Gain proficiency in evaluating network structure through the analysis of nodes and edges, calculating network diameter, and determining average path length to visualize social networks.
- Study the dynamics of information and influence propagation on networks, including the basic cascade model and strategies for influence maximization.

TEACHING - LEARNING STRATEGY:

Following are some sample strategies that can be incorporate for the Course Delivery

- Chalk and Talk Method/Blended Mode Method
- Power Point Presentation
- Expert Talk/Webinar/Seminar
- Video Streaming/Self-Study/Simulations
- Peer-to-Peer Activities
- Activity/Problem Based Learning
- Case Studies
- MOOC/NPTEL Courses
- Any other innovative initiatives with respect to the Course contents

COURSE CONTENTS

MODULE - I	
Introduction to social network analysis and Descriptive network analysis: Introduction to new science of networks. Networks examples. Graph theory basics. Statistical network properties. Degree distribution, clustering coefficient. Frequent patterns. Network motifs. Cliques and k-cores.	**8 Hours**
MODULE - II	
Network structure, Node centralities and ranking on network: Nodes and edges, network diameter and average path length. Node centrality metrics: degree, closeness and betweenness centrality. Eigenvector centrality and PageRank. Algorithm HITS.	**8 Hours**
MODULE - III	
Network communities and Affiliation networks: Networks communities. Graph partitioning and cut metrics. Edge betweenness. Modularity clustering. Affiliation network and bipartite graphs. 1-mode projections. Recommendation systems.	**8 Hours**
MODULE - IV	
Information and influence propagation on networks and Network visualization: Social Diffusion. Basic cascade model. Influence maximization. Most influential nodes in network. Network visualization and graph layouts. Graph sampling. Low -dimensional projections.	**8 Hours**

MODULE - V	
Social media mining and SNA in real world: FB/VK and Twitter analysis: Natural language processing and sentiment mining. Properties of large social networks: friends, connections, likes, re-tweets.	**8 Hours**

COURSE OUTCOMES

Upon completion of this course, the students will be able to:

CO No.	Course Outcome Description	Bloom's Taxonomy Level
CO1	Demonstrate proficiency in applying the principles of the new science of networks, exemplifying their understanding through the identification and analysis of network structures.	CL2
CO2	Evaluate and apply advanced concepts in social network analysis, for comprehensive understanding of network structures and node centrality metrics.	CL3
CO3	Analyze and differentiate various network community detection techniques.	CL3
CO4	Analyze network structures by identifying and justifying the significance of the most influential nodes and show proficiency in using network visualization tools.	CL3
CO5	Evaluate and apply advanced techniques, including natural language processing and sentiment mining, to analyze Facebook, VK, and Twitter data.	CL3

CO-PO-PSO MAPPING

CO No.	Programme Outcomes (PO)												Programme Specific Outcome (PSO)		
	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3
CO1	3	3	2	1				2				2	3		3
CO2	3	3	2					2				2	1	2	1
CO3	3	3	3					2				2	1	3	2
CO4	3	3	3					2				2	1	1	2
CO5	3	3	3					2				2	1	3	2

3: Substantial (High)	2: Moderate (Medium)	1: Poor (Low)

ASSESSMENT STRATEGY

Assessment will be both CIA and SEE. Students learning will be assessed using Direct and Indirect methods:

Sl. No.	Assessment Description	Weightage (%)	Max. Marks
1	**Continuous Internal Assessment (CIA)**	**100 %**	**50**
	Continuous Internal Evaluation (CIE)	60 %	30
	Assignments	40 %	20
2	**Semester End Examination (SEE)**	**100 %**	**50**

ASSESSMENT DETAILS

Continuous Internal Assessment (CIA) (50%)				Semester End Exam (SEE) (50%)
Continuous Internal Evaluation (CIE) (60%)			Assignment/ Activities (40%)	
I	II	III		
Syllabus Coverage			Syllabus Coverage	Syllabus Coverage
40%	30%	30%	100%	100%
MI			MI	MI
MII	MII		MII	MII
	MIII		MIII	MIII

		MIV	MIV	MIV
		MV	MV	MV

Note: For Examinations (both CIE and SEE), the question papers shall contain the questions mapped to the appropriate Bloom's Level. Any COs mapped with higher cognitive Bloom's Level may also be assessed through the assignments.

ASSIGNMENT TYPES WITH WEIGHTAGES

Sl. No.	Assignment Description	Max. Weightage (%)	Max. Marks
1	Written Assignments	25 %	05
2	Quiz	10 %	02
3	Case Studies	25 %	05
4	Seminar/Presentation	15 %	03
5	Peer - to - Peer Learning	10 %	02
6	Activity Based Learning	50 %	10
7	Project Based Learning	50 %	10
8	Field Work + Report	50 %	10
9	Industry Visit + Report	50 %	10
10	NPTEL/MOOC Courses – Registration and Assignment Submissions	50 %	10
	NPTEL Certification	75 %	15
11	Any other Innovative Assignments (CL4 and above)	50 %	10

Note: The assignments mentioned above may be provided appropriately to the students belonging to different bands

SEE QUESTION PAPER PATTERN:

- The question paper will have **TEN** full questions from **FIVE** Modules
- There will be 2 full questions from each module. Every question will carry a maximum of 20 marks.
- Each full question may have a maximum of four sub-questions covering all the topics under a module.
- The students will have to answer FIVE full questions, selecting one full question from each module.

TEXT BOOKS:

1. David Easley and John Kleinberg. "Networks, Crowds, and Markets: Reasoning About a Highly Connected World." Cambridge University Press 2010.
2. Eric Kolaczyk, Gabor Csardi. Statistical Analysis of Network Data with R (Use R!). Springer, 2014
3. Stanley Wasserman and Katherine Faust. "Social Network Analysis. Methods and Applications." Cambridge University Press, 1994.
4. Guandong Xu ,Yanchun Zhang and Lin Li, ―Web Mining and Social Networking – Techniques and applications‖, First Edition, Springer, 2011.
5. Dion Goh and Schubert Foo, ―Social information Retrieval Systems: Emerging Technologies and Applications for Searching the Web Effectively‖, IGI Global Snippet, 2008.
6. Max Chevalier, Christine Julien and Chantal Soulé-Dupuy, ―Collaborative and Social Information Retrieval and Access: Techniques for Improved user Modelling‖, IGI Global Snippet, 2009.
7. John G. Breslin, Alexander Passant and Stefan Decker, ―The Social Semantic Web‖, Springer, 2009.

REFERENCE WEB LINKS AND VIDEO LECTURES (E - RESOURCES):

1. https://onlinecourses.nptel.ac.in/noc22_cs117/preview

BIOMETRICS AND SECURITY

(Effective from the Academic Year 2023 - 2024)

VI SEMESTER

Course Code	**21CY644**	CIA Marks	50
Number of Contact Hours/Week (L: T: P: S)	3:0:0:0	SEE Marks	50
Total Hours of Pedagogy	**40L**	Exam Hours	03

CREDITS – 4

COURSE PREREQUISITES:

- Basic of computer science and programming,
- Basic of Linear Algebra and Statistics

COURSE OBJECTIVES:

- Explain the general principles of designing biometric-based systems.
- Analyze various biometric systems, their characteristics and performance
- Discuss the online identification biometric techniques
- Recognize some of the personal privacy and security implications of biometrics-based identification technology.
- Analyze the privacy and security issues of biometrics.

TEACHING - LEARNING STRATEGY:

- Following are some sample strategies that can be incorporate for the Course Delivery
- Chalk and Talk Method/Blended Mode Method
- Power Point Presentation
- Expert Talk/Webinar/Seminar
- Video Streaming/Self-Study/Simulations
- Peer-to-Peer Activities
- Activity/Problem Based Learning
- Case Studies
- MOOC/NPTEL Courses
- Any other innovative initiatives with respect to the Course contents

COURSE CONTENTS

MODULE -1

Introduction to Biometrics: Introduction, Identification Methods, Biometrics, Biometrics Technology Overview, Biometrics technologies: A Comparison, Automatic Identification, Research Issues, Acquisition, Representation, Feature Extraction, Matching, Search, Organization and Scalability, Privacy, Novel Applications.	**8 Hours**

MODULE -2

Finger Print Verification: Matching, Verification and Identification, Feature type, Image Processing and Verification, System Issues, Recognition Rate. **Face Recognition:** Introduction, Approaches, The Design of a face recognition system, Face Detection, Feature Extraction and Matching.	**8 Hours**

MODULE -3

Hand Geometry Base Verification: Introduction, System Operation, Implementation Issues, Applications. **Recognizing By Iris Patterns:** Introduction, Iris Patterns, Complex Phenotypic Features, Statistical Recognition Principle, Decidability of Iris Based personal Identification, Identification versus Verification, Stability of Iris Pattern Overtime.	**8 Hours**

MODULE -4	
Retina Identification: Retina/Choroid as Human Descriptor, Background, Technology, Eye Signature, RI Camera, Signal Acquisition and Computing Subsystem, System Operation, Performance. **Key stroke Dynamics Based Authentication:** Introduction, Types of Security Attacks, Predicting Human Characteristics, Applications of Keystroke Dynamics using Interkey Times and Hold Times as Features.	**8 Hours**
MODULE -5	
Multimodal Biometrics: Introduction to multimodal biometric, Limitations of Unimodal Biometric system, Multimodal Fusion Techniques, Performance Metrics and Evaluation, Security and Privacy Concerns, Emerging technologies. **Biometrics: Identifying Law & Policy Concerns:** Introduction, Definition and Advantages, Biometric Applications, Context of Biometrics, Privacy Concerns, Biometric Centralization vs. Biometric Balkanization.	**8 Hours**

COURSE OUTCOMES

Upon completion of this course, the students will be able to:

CO No.	Course Outcome Description	Bloom's Taxonomy Level
CO1	Explain the general principles of designing biometric-based systems.	CL2
CO2	Design Fingerprint verification and Face recognition system.	CL3
CO3	Design hand geometry Based Verification and Iris patterns detection system	CL3
CO4	Design Retina Identification and Keystroke Dynamics Based Authentication	CL3
CO5	Understand the multi modal Biometrics and understand law and policy concerns in biometrics.	CL2

CO-PO-PSO MAPPING

CO No.	Programme Outcomes (PO)												Programme Specific Outcome (PSO)		
	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3
CO1	3	3	3	2	2							2	2	2	2
CO2	3	3	3	2	2							2	2	2	2
CO3	3	3	3	2	2							2	2	2	2
CO4	3	3	3	2	2							2	2	2	2
CO5	3	3	3	2	2							2	2	2	2

3: Substantial (High) | **2: Moderate (Medium)** | **1: Poor (Low)**

ASSESSMENT STRATEGY

Assessment will be both CIA and SEE. Students learning will be assessed using Direct and Indirect methods:

Sl. No.	Assessment Description	Weightage (%)	Max. Marks
1	**Continuous Internal Assessment (CIA)**	**100 %**	**50**
	Continuous Internal Evaluation (CIE)	60 %	30
	Assignments	40 %	20
2	**Semester End Examination (SEE)**	**100 %**	**50**

ASSESSMENT DETAILS				
Continuous Internal Assessment (CIA) (50%)				Semester End Exam (SEE) (50%)
Continuous Internal Evaluation (CIE) (60%)			Assignment/Activities (40%)	
I	II	III		
Syllabus Coverage			Syllabus Coverage	Syllabus Coverage
40%	30%	30%	100%	100%
MI			MI	MI
MII	MII		MII	MII
	MIII		MIII	MIII
		MIV	MIV	MIV
		MV	MV	MV

Note: For Examinations (both CIE and SEE), the question papers shall contain the questions mapped to the appropriate Bloom's Level. Any COs mapped with higher cognitive Bloom's Level may also be assessed through the assignments.

ASSIGNMENT TYPES WITH WEIGHTAGES

Sl. No.	Assignment Description	Max. Weightage (%)	Max. Marks
1	Written Assignments	25 %	05
2	Quiz	10 %	02
3	Case Studies	25 %	05
4	Seminar/Presentation	15 %	03
5	Peer - to - Peer Learning	10 %	02
6	Activity Based Learning	50 %	10
7	Project Based Learning	50 %	10
8	Field Work + Report	50 %	10
9	Industry Visit + Report	50 %	10
10	NPTEL/MOOC Courses – Registration and Assignment Submissions	50 %	10
	NPTEL Certification	75 %	15
11	Any other Innovative Assignments (CL4 and above)	50 %	10

Note: The assignments mentioned above may be provided appropriately to the students belonging to different bands

SEE QUESTION PAPER PATTERN:

- The question paper will have **TEN** full questions from **FIVE** Modules
- There will be 2 full questions from each module. Every question will carry a maximum of 20 marks.
- Each full question may have a maximum of four sub-questions covering all the topics under a module.
- The students will have to answer FIVE full questions, selecting one full question from each module.

TEXT BOOKS:

1. "Biometrics, Personal Identification in Networked Society", Anil Jain, Ruud Bolle, Sharath Pankanti, Kluwer Academic Publishers, 2002
2. "Biometrics -Identity verification in a networked World", Samir Nanavathi, Michel Thieme, and Raj Nanavathi, Wiley Eastern, 2002.
3. "Implementing Biometric Security", John Chirillo and Scott Blaul, Wiley Eastern Publications, 2005.
4. "Biometrics for Network Security", John Berger, Prentice Hall, 2004.

SAHYADRI
COLLEGE OF ENGINEERING & MANAGEMENT
An Autonomous Institution
MANGALURU

BLOCKCHAIN & APPLICATIONS

(Effective from the Academic Year 2023 - 2024)

VI SEMESTER

Course Code:	**21CS651**	CIA Marks	50
Number of Contact Hours/Week (L: T: P: S)	3:0:0:0	SEE Marks	50
Total Hours of Pedagogy	**40L**	Exam Hours	03

CREDITS – 3

COURSE PREREQUISITES:

- Fundamental knowledge of Mathematics, Data Structures, Networking

COURSE OBJECTIVES:

- Define and explain the fundamentals of Block chain
- Illustrate the technologies of Block chain
- Describe the models of Block chain
- Analyze and demonstrate the Ethereum

TEACHING - LEARNING STRATEGY:

Following are some sample strategies that can be incorporate for the Course Delivery

- Chalk and Talk Method/Blended Mode Method
- Power Point Presentation
- Expert Talk/Webinar/Seminar
- Video Streaming/Self-Study/Simulations
- Peer-to-Peer Activities
- Activity/Problem Based Learning
- Case Studies
- MOOC/NPTEL Courses
- Any other innovative initiatives with respect to the Course contents

COURSE CONTENTS

MODULE - I

Introduction to Blockchain Technology: Distributed systems, The history of blockchain, CAP theorem and blockchain, Benefits and limitations of blockchain, Decentralization using blockchain, Methods of decentralization, Routes to decentralization.	**8 Hours**

MODULE - II

Cryptography in Blockchain: Introduction, cryptographic primitives, Asymmetric cryptography, public and private keys, RSA, ECC, Hash functions, financial markets and trading	**8 Hours**

MODULE - III

Bit Coin Introduction, Transactions: Structure, Transactions types, The structure of a block, The genesis block, The bitcoin network, Wallets and its types, Bitcoin payments, Bitcoin investment and buying and selling bitcoins, Bitcoin installation, Bitcoin programming and the command-line interface, Bitcoin improvement proposals (BIPs).	**8 Hours**

MODULE - IV

Ethereum: Ethereum block chain, Ethereum network, Components of the Ethereum ecosystem, Keys and Addresses, Accounts and its types, Transactions and Messages, Contract Creation transaction, Message call transaction, messages, Calls, Transaction Validation and execution, Transaction substrate, State storage in the Ethereum blockchain, Ether cryptocurrency / tokens (ETC and ETH), The Ethereum Virtual Machine (EVM), Execution environment, Native contracts.	**8 Hours**

MODULE – V

Smart Contract and Hyper ledger: Ricardian contracts, Application developed on Etherium : The DAO. **Hyper ledger:** Hyper ledger projects, Hyperledger as a protocol, The reference architecture, Requirements and design goals of Hyperledger Fabric, Applications on blockchain on fabric, Consensus in Hyperledger Fabric, The transaction life cycle in Hyperledger Fabric, Sawtooth Lake, Corda Architecture.	**8 Hours**

COURSE OUTCOMES

Upon completion of this course, the students will be able to:

CO No.	Course Outcome Description	Bloom's Taxonomy Level
CO1	Apply basic concepts of Blockchain and evaluate the benefits and limitation of Blockchain	CL3
CO2	Examine the decentralization concepts and apply the cryptography techniques in Blockchain	CL3
CO3	Demonstrate the structure, usage, wallet transaction and installation of Bitcoin	CL3
CO4	Demonstrate Application development using Ethereum	CL3
CO5	Illustrate the usage of Smart contract and architecture of Hyperledger	CL3

CO-PO-PSO MAPPING

CO No.	Programme Outcomes (PO)												Programme Specific Outcome (PSO)		
	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3
CO1	3	3	2						1		2	2	2	1	1
CO2	3	3	2						1		2	2	2	1	1
CO3	3	3	2		2				1		2	2	2	1	1
CO4	3	3	2		2				1		2	2	2	1	1
CO5	3	3	2		2				1		2	2	2	1	1
3: Substantial (High)					**2: Moderate (Medium)**					**1: Poor (Low)**					

ASSESSMENT STRATEGY

Assessment will be both CIA and SEE. Students learning will be assessed using Direct and Indirect methods:

Sl. No.	Assessment Description	Weightage (%)	Max. Marks
1	**Continuous Internal Assessment (CIA)**	**100 %**	**50**
	Continuous Internal Evaluation (CIE)	60 %	30
	Assignments	40 %	20
2	**Semester End Examination (SEE)**	**100 %**	**50**

ASSESSMENT DETAILS

Continuous Internal Assessment (CIA) (50%)				Semester End Exam (SEE) (50%)
Continuous Internal Evaluation (CIE) (60%)			Assignment/ Activities (40%)	
I	II	III		
Syllabus Coverage			Syllabus Coverage	Syllabus Coverage
40%	30%	30%	100%	100%
MI			MI	MI
MII	MII		MII	MII
	MIII		MIII	MIII
		MIV	MIV	MIV
		MV	MV	MV

Note: For Examinations (both CIE and SEE), the question papers shall contain the questions mapped to the appropriate Bloom's Level. Any COs mapped with higher cognitive Bloom's Level may also be assessed through the assignments.

ASSIGNMENT TYPES WITH WEIGHTAGES

Sl. No.	Assignment Description	Max. Weightage (%)	Max. Marks
1	Written Assignments	25 %	05
2	Quiz	10 %	02
3	Case Studies	25 %	05
4	Seminar/Presentation	15 %	03
5	Peer - to - Peer Learning	10 %	02
6	Activity Based Learning	50 %	10
7	Project Based Learning	50 %	10
8	Field Work + Report	50 %	10
9	Industry Visit + Report	50 %	10
10	NPTEL/MOOC Courses – Registration and Assignment Submissions	50 %	10
	NPTEL Certification	75 %	15
11	Any other Innovative Assignments (CL4 and above)	50 %	10

Note: The assignments mentioned above may be provided appropriately to the students belonging to different bands

SEE QUESTION PAPER PATTERN:

- The question paper will have **TEN** full questions from **FIVE** Modules
- There will be 2 full questions from each module. Every question will carry a maximum of 20 marks.
- Each full question may have a maximum of four sub-questions covering all the topics under a module.
- The students will have to answer FIVE full questions, selecting one full question from each module.

TEXT BOOKS:

1. Bashir, Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained, 2nd Edition, 2nd Revised edition. Birmingham: Packt Publishing, 2018.
2. A. M. Antonopoulos, Mastering bitcoin, First edition. Sebastopol CA: O'Reilly,2015.
3. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, ―An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends in 2017 IEEE International Congress on Big Data (Bigdata Congress), 2017, pp.557–564

REFERENCE WEB LINKS AND VIDEO LECTURES (E - RESOURCES):

1. https://ethereum.org/en/
2. https://www.blockchain.com/explorer

CLOUD COMPUTING AND ITS APPLICATION

(Effective from the Academic Year 2023 - 2024)

VI SEMESTER

Course Code	**21AI652**	CIA Marks	50
RT	3:0:0:0	SEE Marks	50
Total Hours of Pedagogy	**40L**	Exam Hours	03

CREDITS – 3

COURSE PREREQUISITES:

- Fundamental knowledge of computer networks.

COURSE OBJECTIVES:

- Provide students with the fundamentals and essentials of Cloud Computing.
- To provide students a sound foundation of Cloud Computing so that they are able to start using and adopting Cloud Computing services and tools in their real-life scenarios.
- To enable students exploring some important cloud computing driven commercial systems and applications.
- To expose the students to frontier areas of Cloud Computing and information systems, while providing sufficient foundations to enable further study and research.

TEACHING - LEARNING STRATEGY:

Following are some sample strategies that can be incorporate for the Course Delivery

- Chalk and Talk Method/Blended Mode Method
- Power Point Presentation
- Expert Talk/Webinar/Seminar
- Video Streaming/Self-Study/Simulations
- Peer-to-Peer Activities
- Activity/Problem Based Learning
- Case Studies
- MOOC/NPTEL Courses
- Any other innovative initiatives with respect to the Course contents

COURSE CONTENTS

MODULE - I

Introduction: Cloud Computing at a Glance, The Vision of Cloud Computing, Defining a Cloud, A Closer Look, Cloud Computing Reference Model, Characteristics and Benefits, Challenges Ahead, Historical Developments, Distributed Systems, Virtualization, Web 2.0, Service-Oriented Computing, Utility-Oriented Computing, Building Cloud Computing Environments, Application Development, Infrastructure and System Development, Computing Platforms and Technologies. **Virtualization**: Introduction, Characteristics of Virtualized, Environments Taxonomy of Virtualization Techniques, Execution Virtualization, Other Types of Virtualization, Virtualization and Cloud Computing, Pros and Cons of Virtualization, Technology Examples Xen: Paravirtualization, VMware: Full Virtualization, Microsoft Hyper-V	**8 Hours**

MODULE – II

Cloud Computing Architecture: Introduction, Cloud Reference Model, Architecture, Infrastructure / Hardware as a Service, Platform as a Service, Software as a Service, Types of Clouds, Public Clouds, Private Clouds, Hybrid Clouds, Community Clouds, Economics of the Cloud, Open Challenges, Cloud Definition, Cloud Interoperability and Standards Scalability and Fault Tolerance Security, Trust, and Privacy Organizational Aspects **Aneka:** Cloud Application Platform, Framework Overview, Anatomy of the Aneka Container, From the Ground Up: Platform Abstraction Layer, Fabric Services, foundation Services, Application Services, Building	**8 Hours**

Aneka Clouds, Infrastructure Organization, Logical Organization, Private Cloud Deployment Mode, Public Cloud Deployment Mode. Case study: Netflix	

MODULE - III

Concurrent Computing: Introducing Parallelism for Single Machine Computation, Programming Applications with Threads, What is a Thread?, Thread APIs, Techniques for Parallel Computation with Threads, Multithreading with Aneka, Introducing the Thread Programming Model, Aneka Thread vs. Common Threads, Programming Applications with Aneka Threads, Aneka Threads Application Model, Domain Decomposition: Matrix Multiplication, Functional Decomposition: Sine, Cosine, and Tangent.	**8 Hours**

MODULE - IV

Data-Intensive Computing: What is Data-Intensive Computing?, Characterizing Data-Intensive Computations, Challenges Ahead, Historical Perspective, Technologies for Data-Intensive Computing, Storage Systems, Programming Platforms, Aneka MapReduce Programming, Introducing the MapReduce Programming Model, Example Application Exploring Large-Data Issues in the Curriculum: A Case Study with MapReduce.	**8 Hours**

MODULE - V

Cloud Platforms in Industry: Amazon Web Services, Compute Services, Storage Services, Communication Services, Additional Services, Google AppEngine, Architecture and Core Concepts, Application Life-Cycle, Cost Model, Observations, Microsoft Azure, Azure Core Concepts, SQL Azure, Windows Azure Platform Appliance. **Cloud Applications**: Scientific Applications, Healthcare: ECG Analysis in the Cloud, Biology: Protein Structure Prediction, Biology: Gene Expression Data Analysis for Cancer Diagnosis, Geoscience: Satellite Image Processing, Business and Consumer Applications, CRM and ERP, Productivity, Social Networking, Media Applications, Multiplayer Online Gaming.	**8 Hours**

COURSE OUTCOMES

Upon completion of this course, the students will be able to:

CO No.	Course Outcome Description	Bloom's Taxonomy Level
CO1	Explain cloud computing, virtualization and classify services of cloud computing	CL3
CO2	Illustrate architecture and programming in c loud	CL3
CO3	Able to use concurrent programming methods	CL3
CO4	Able to use data intensive services like map reduce	CL3
CO5	Describe the platforms for development of cloud applications and list the application of cloud.	CL3

CO-PO-PSO MAPPING

CO No.	Programme Outcomes (PO)												Programme Specific Outcome (PSO)		
	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3
CO1	3	3	2	1				2				2	2	2	2
CO2	3	3	2					2				2	2	2	2
CO3	3	3	3					2				2	2	2	2
CO4	3	3	3					2				2	2	2	2
CO5	3	3	3					2				2	2	2	2

3: Substantial (High) | **2: Moderate (Medium)** | **1: Poor (Low)**

ASSESSMENT STRATEGY

Assessment will be both CIA and SEE. Students learning will be assessed using Direct and Indirect methods:

Sl. No.	Assessment Description	Weightage (%)	Max. Marks
1	**Continuous Internal Assessment (CIA)**	**100 %**	**50**
	Continuous Internal Evaluation (CIE)	60 %	30
	Assignments	40 %	20
2	**Semester End Examination (SEE)**	**100 %**	**50**

ASSESSMENT DETAILS

Continuous Internal Assessment (CIA) (50%)				
Continuous Internal Evaluation (CIE) (60%)			**Assignment/ Activities (40%)**	**Semester End Exam (SEE) (50%)**
I	**II**	**III**		
Syllabus Coverage			**Syllabus Coverage**	**Syllabus Coverage**
40%	**30%**	**30%**	**100%**	**100%**
MI			MI	MI
MII	MII		MII	MII
	MIII		MIII	MIII
		MIV	MIV	MIV
		MV	MV	MV

Note: For Examinations (both CIE and SEE), the question papers shall contain the questions mapped to the appropriate Bloom's Level. Any COs mapped with higher cognitive Bloom's Level may also be assessed through the assignments.

ASSIGNMENT TYPES WITH WEIGHTAGES

Sl. No.	Assignment Description	Max. Weightage (%)	Max. Marks
1	Written Assignments	25 %	05
2	Quiz	10 %	02
3	Case Studies	25 %	05
4	Seminar/Presentation	15 %	03
5	Peer - to - Peer Learning	10 %	02
6	Activity Based Learning	50 %	10
7	Project Based Learning	50 %	10
8	Field Work + Report	50 %	10
9	Industry Visit + Report	50 %	10
10	NPTEL/MOOC Courses – Registration and Assignment Submissions	50 %	10
	NPTEL Certification	75 %	15
11	Any other Innovative Assignments (CL4 and above)	50 %	10

Note: The assignments mentioned above may be provided appropriately to the students belonging to different bands

SEE QUESTION PAPER PATTERN:

- The question paper will have **TEN** full questions from **FIVE** Modules
- There will be 2 full questions from each module. Every question will carry a maximum of 20 marks.
- Each full question may have a maximum of four sub-questions covering all the topics under a module.
- The students will have to answer FIVE full questions, selecting one full question from each module.

TEXT BOOKS:

1. Rajkumar Buyya, Christian Vecchiola, and Thamarai Selvi Mastering Cloud. Computing McGraw Hill Education
2. Dan C. Marinescu, Cloud Computing Theory and Practice, Morgan Kaufmann, Elsevier 2013.

REFERENCE WEB LINKS AND VIDEO LECTURES (E - RESOURCES):

1. What is Cloud Computing? | Amazon Web Services - YouTube https://youtu.be/mxT233EdY5c

SAHYADRI
COLLEGE OF ENGINEERING & MANAGEMENT
An Autonomous Institution
MANGALURU

PARALLEL COMPUTING

(Effective from the Academic Year 2023 - 2024)

VI SEMESTER

Course Code	**21CS653**	CIA Marks	50
Number of Contact Hours/Week (L: T: P: S)	3:0:0:0	SEE Marks	50
Total Hours of Pedagogy	**40L**	Exam Hours	03

CREDITS – 3

COURSE PREREQUISITES:

- Fundamental knowledge of OS, Data Structures.

COURSE OBJECTIVES:

- Introduce students the design, analysis, and implementation, of high performance computational science and engineering applications.
- Illustrate on advanced computer architectures, parallel algorithms, parallel languages, and performance-oriented computing.

TEACHING - LEARNING STRATEGY:

Following are some sample strategies that can be incorporate for the Course Delivery

- Chalk and Talk Method/Blended Mode Method
- Power Point Presentation
- Expert Talk/Webinar/Seminar
- Video Streaming/Self-Study/Simulations
- Peer-to-Peer Activities
- Activity/Problem Based Learning
- Case Studies
- MOOC/NPTEL Courses
- Any other innovative initiatives with respect to the Course contents

COURSE CONTENTS

MODULE – I

Introduction to Parallel Computing: Motivating Parallelism, Scope of Parallel Computing, **Parallel Programming Platforms:** Implicit Parallelism: Trends in Microprocessor Architectures, Limitations of Memory System Performance, Dichotomy of Parallel Computing Platforms, Physical Organization of Parallel Platforms, Communication Costs in Parallel Machines, Routing Mechanisms for Interconnection Networks, Impact of Process-Processor Mapping and Mapping Techniques.	**8 Hours**

MODULE – II

Principles of Parallel Algorithm Design: Preliminaries, Decomposition Techniques, Characteristics of Tasks and Interactions, Mapping Techniques for Load Balancing, Methods for Containing Interaction Overheads, Parallel Algorithm Models **Basic Communication Operations:** One-to-All Broadcast and All-to-One Reduction, All to-All Broadcast and Reduction, All-Reduce and Prefix-Sum Operations, Scatter and Gather, All-to-All Personalized Communication, Circular Shift, Improving the Speed of Some Communication Operations	**8 Hours**

MODULE – III

Analytical Modeling of Parallel Programs: Sources of Overhead in Parallel Programs, Performance Metrics for Parallel Systems, The Effect of Granularity on Performance, Scalability of Parallel Systems. Minimum Execution Time and Minimum Cost-Optimal Execution Time, Asymptotic Analysis of Parallel Programs. Other Scalability Metrics, Programming Using the Message-Passing Paradigm: Principles of Message-Passing Programming, The Building Blocks: Send and Receive Operations, MPI: the Message Passing Interface, Topologies and Embedding, Overlapping Communication with Computation, Collective Communication and Computation Operations, Groups and Communicators.	**8 Hours**

MODULE – IV	
Programming Shared Address Space Platforms: Thread Basics, Why Threads?, The POSIX Thread API, Thread Basics: Creation and Termination, Synchronization Primitives in Pthreads, Controlling Thread and Synchronization Attributes, Thread Cancellation, Composite Synchronization Constructs, Tips for Designing Asynchronous Programs, OpenMP: a Standard for Directive Based Parallel Programming, Dense Matrix Algorithms: Matrix-Vector Multiplication, Matrix-Matrix Multiplication, Solving a System of Linear Equations, Sorting: Issues in Sorting on Parallel Computers, Sorting Networks, Bubble Sort and its Variants.	**8 Hours**
MODULE – V	
Graph Algorithms: Definitions and Representation, Minimum Spanning Tree: Prim's Algorithm, Single-Source Shortest Paths: Dijkstra's Algorithm, All-Pairs Shortest Paths, Transitive Closure, Connected Components, Algorithms for Sparse Graphs, Search Algorithms for Discrete Optimization Problems: Definitions and Examples, Sequential Search Algorithms, Search Overhead Factor, Parallel Depth-First Search, Parallel Best-First Search, Speedup, Anomalies in Parallel Search Algorithms.	**8 Hours**

COURSE OUTCOMES

Upon completion of this course, the students will be able to:

CO No.	Course Outcome Description	Bloom's Taxonomy Level
CO1	Demonstrate understanding of Parallel Computing Ecosystem.	CL2
CO2	Showcase expertise in parallel algorithm design by developing a robust understanding of parallel algorithm models and their implications on design.	CL3
CO3	Identify and analyze sources of overhead in parallel programs, recognizing their impact on performance; assess performance metrics for parallel systems, gaining expertise in MPI.	CL4
CO4	Master Thread-Based Parallel Programming, utilizing the OpenMP Standard for directive-based parallel programming, with a focus on dense matrix algorithms and addressing challenges in sorting on parallel computers.	CL4
CO5	Excel in Graph Algorithm by demonstrating proficiency in both sequential and parallel search algorithms.	CL4

CO-PO-PSO MAPPING

CO No.	Programme Outcomes (PO)												Programme Specific Outcome (PSO)		
	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3
CO1	3	3	3		2	2			2	1	1	3	3	3	3
CO2	3	3	3		2		1	1	2	1	1	3	3	3	3
CO3	3	3	3		2				2	1	1	3	3	3	3
CO4	3	3	3		2				2	1	1	3	3	3	3
CO5	3	3	3		2				2	1	1	3	3	3	3
3: Substantial (High)					**2: Moderate (Medium)**					**1: Poor (Low)**					

ASSESSMENT STRATEGY

Assessment will be both CIA and SEE. Students learning will be assessed using Direct and Indirect methods:

Sl. No.	Assessment Description	Weightage (%)	Max. Marks
1	**Continuous Internal Assessment (CIA)**	**100 %**	**50**
	Continuous Internal Evaluation (CIE)	60 %	30
	Assignments	40 %	20
2	**Semester End Examination (SEE)**	**100 %**	**50**

ASSESSMENT DETAILS

Continuous Internal Assessment (CIA) (50%)				
Continuous Internal Evaluation (CIE) (60%)			Assignment/ Activities (40%)	Semester End Exam (SEE) (50%)
I	II	III		
Syllabus Coverage			Syllabus Coverage	Syllabus Coverage
40%	30%	30%	100%	100%
MI			MI	MI
MII	MII		MII	MII
	MIII		MIII	MIII
		MIV	MIV	MIV
		MV	MV	MV

Note: For Examinations (both CIE and SEE), the question papers shall contain the questions mapped to the appropriate Bloom's Level. Any COs mapped with higher cognitive Bloom's Level may also be assessed through the assignments.

ASSIGNMENT TYPES WITH WEIGHTAGES

Sl. No.	Assignment Description	Max. Weightage (%)	Max. Marks
1	Written Assignments	25 %	05
2	Quiz	10 %	02
3	Case Studies	25 %	05
4	Seminar/Presentation	15 %	03
5	Peer - to - Peer Learning	10 %	02
6	Activity Based Learning	50 %	10
7	Project Based Learning	50 %	10
8	Field Work + Report	50 %	10
9	Industry Visit + Report	50 %	10
10	NPTEL/MOOC Courses – Registration and Assignment Submissions	50 %	10
	NPTEL Certification	75 %	15
11	Any other Innovative Assignments (CL4 and above)	50 %	10

Note: The assignments mentioned above may be provided appropriately to the students belonging to different bands

SEE QUESTION PAPER PATTERN:

- The question paper will have **TEN** full questions from **FIVE** Modules
- There will be 2 full questions from each module. Every question will carry a maximum of 20 marks.
- Each full question may have a maximum of four sub-questions covering all the topics under a module.
- The students will have to answer FIVE full questions, selecting one full question from each module.

TEXT BOOKS:

1. Introduction to Parallel Computing, Ananth Grama, Anshul Gupta, George Karypis, and Vipin Kumar, 2nd edition, Addison-Welsey, 2003.
2. Grama, A. Gupta, G. Karypis, V. Kumar, An Introduction to Parallel Computing, Design and Analysis of Algorithms: 2/e, Addison-Wesley, 2003.
3. G.E. Karniadakis, R.M. Kirby II, Parallel Scientific Computing in C++ and MPI: A Seamless Approach to Parallel Algorithms and their Implementation, Cambridge University Press,2003.
4. Wilkinson and M. Allen, Parallel Programming: Techniques and Applications Using Networked Workstations and Parallel Computers, 2/E, Prentice Hall, 2005.
5. M.J. Quinn, Parallel Programming in C with MPI and OpenMP, McGraw-Hill, 2004.
6. G.S. Almasi and A. Gottlieb, Highly Parallel Computing, 2/E, Addison-Wesley, 1994.

7. David Culler Jaswinder Pal Singh,"Parallel Computer Architecture: A hardware/Software Approach", Morgan Kaufmann, 1999.
8. Kai Hwang, "Scalable Parallel Computing", McGraw Hill 1998.

SAHYADRI
COLLEGE OF ENGINEERING & MANAGEMENT
An Autonomous Institution
MANGALURU

ADVANCED PROTOCOL ENGINEERING

(Effective from the Academic Year 2022 - 2023)

VI SEMESTER

Course Code	**21CY654**	CIA Marks	50
Number of Contact Hours/Week (L: T: P: S)	3:0:0:0	SEE Marks	50
Total Hours of Pedagogy	**40L**	Exam Hours	03

CREDITS – 3

COURSE PREREQUISITES:

- It is recommended that students have a background in computer communication system.

COURSE OBJECTIVES:

- Evaluate networking protocols in AP notation
- Compare and contrast on routing, security and compression protocols
- Designing various error and congestion and multiplexing protocols

TEACHING - LEARNING STRATEGY:

Following are some sample strategies that can be incorporate for the Course Delivery

- Chalk and Talk Method/Blended Mode Method
- PowerPoint Presentation
- Expert Talk/Webinar/Seminar
- Video Streaming/Self-Study/Simulations
- Peer-to-Peer Activities
- Activity/Problem Based Learning
- Case Studies
- MOOC/NPTEL Courses
- Any other innovative initiatives with respect to the Course contents

COURSE CONTENTS

MODULE-1	
Network protocols: Network protocols, Semantics of traditional protocol specifications, syntax of traditional protocol. Network processes constants, inputs, and variables. Specifications in new protocol, A vending machine protocol, a request/reply protocol, a Manchester encoding protocol, Current internet.	**8 Hours**
MODULE -2	
Network Process: Protocol execution processes in the internet, Nondeterministic assignment process arrays, protocol process communication in the internet, Types of transmission errors, Error occurrence. Normal timeout actions implementing transmission errors in the internet connections: using timeouts connections, using identifiers full-duplex and half-duplex connections, Connections in the internet.	**8 Hours**
MODULE – 3	
Error detection, recovery and flow control: Detection of message corruption, Detection of message loss, detection of message reorder, error detection in the internet. Error recovery-forward & backward error recovery. Cumulative acknowledgment, individual acknowledgment, blocks acknowledgment error recovery in the internet, flow control. Window size control, rate control, circular buffer control, flow control in the internet.	**8 Hours**
MODULE-4	
Topology Information: Local and global topology information, Maintaining local topology information, Hierarchical topology information, Topology information in the internet, Abstraction of perfect channel in the internet, Hierarchical routing, random routing.	**8 Hours**

MODULE-5	
Security and Data Compression: Asymmetric and symmetric keys authentication, Privacy and integrity non-repudiation authorization, Message digest security in the internet data compression, Huffman coding, static Huffman compression, dynamic Huffman compression, Context sensitive compression, lossy compression, data compression in the internet.	**8 Hours**

COURSE OUTCOMES

Upon completion of this course, the students will be able to:

CO No.	Course Outcome Description	Bloom's Taxonomy Level
CO1	Understand Specification of network protocols	CL2
CO2	Understand Protocol execution process and types of errors	CL2
CO3	Design various error recovery and flow control	CL3
CO4	Illustrate the topology information and routing techniques	CL3
CO5	Understand authentication, Privacy and various compression techniques	CL2

CO-PO-PSO MAPPING

CO No.	Programme Outcomes (PO)												Programme Specific Outcome (PSO)		
	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3
CO1	3	3	3		2							2	2	2	2
CO2	3	3	3		2							2	2	2	2
CO3	3	3	3		2							2	2	2	2
CO4	3	3	3		2							2	2	2	2
CO5	3	3	3		2							2	2	2	2
3: Substantial (High)				**2: Moderate (Medium)**					**1: Poor (Low)**						

ASSESSMENT STRATEGY

Assessment will be both CIA and SEE. Students learning will be assessed using Direct and Indirect methods:

Sl. No.	Assessment Description	Weightage (%)	Max. Marks
1	**Continuous Internal Assessment (CIA)**	**100 %**	**50**
	Continuous Internal Evaluation (CIE)	60 %	30
	Assignments	40 %	20
2	**Semester End Examination (SEE)**	**100 %**	**50**

ASSESSMENT DETAILS

Continuous Internal Assessment (CIA) (50%)				**Semester End Exam (SEE) (50%)**
Continuous Internal Evaluation (CIE) (60%)			**Assignment/ Activities (40%)**	
I	**II**	**III**		
Syllabus Coverage			**Syllabus**	

			Coverage	Syllabus Coverage
40%	**30%**	**30%**	**100%**	**100%**
MI			MI	MI
MII	MII		MII	MII
	MIII		MIII	MIII
		MIV	MIV	MIV
		MV	MV	MV

Note: For Examinations (both CIE and SEE), the question papers shall contain the questions mapped to the appropriate Bloom's Level. Any COs mapped with higher cognitive Bloom's Level may also be assessed through the assignments.

ASSIGNMENT TYPES WITH WEIGHTAGES

Sl. No.	Assignment Description	Max. Weightage (%)	Max. Marks
1	Written Assignments	25 %	05
2	Quiz	10 %	02
3	Case Studies	25 %	05
4	Seminar/Presentation	15 %	03
5	Peer - to - Peer Learning	10 %	02
6	Activity Based Learning	50 %	10
7	Project Based Learning	50 %	10
8	Field Work + Report	50 %	10
9	Industry Visit + Report	50 %	10
10	NPTEL/MOOC Courses – Registration and Assignment Submissions	50 %	10
	NPTEL Certification	75 %	15
11	Any other Innovative Assignments (CL4 and above)	50 %	10

Note: The assignments mentioned above may be provided appropriately to the students belonging to different bands

SEE QUESTION PAPER PATTERN:

- The question paper will have **TEN** full questions from **FIVE** Modules
- There will be 2 full questions from each module. Every question will carry a maximum of 20 marks.
- Each full question may have a maximum of four sub-questions covering all the topics under a module.
- The students will have to answer FIVE full questions, selecting one full question from each module.

TEXT BOOKS:

1. Elements of Network Protocol Design, Mohamed G. Gouda, John Wiley & Sons, 2004
2. Computer Networks and Internet with Internet Applications, Douglas E Comer, Pearson, Fourth Edition, 2004

CYBER SECURITY FUNDAMENTALS AND LAWS LABORATORY

(Effective from the Academic Year 2023 - 2024)

VI SEMESTER

Course Code	**21CYL66**	CIA Marks	50
Number of Contact Hours/Week (L: T: P: S)	0:0:2:0	SEE Marks	50
Total Hours of Pedagogy	20P	Exam Hours	03

CREDITS – 1

COURSE PREREQUISITES:

- Basic familiarity with Computer network & security

COURSE OBJECTIVES:

- To configure virtual networks using network simulator
- To install and exploit security tools for protecting a network
- To implement cryptographic algorithm for building a secure communication network
- To exploit the vulnerabilities in a LAN environment to launch attacks

TEACHING - LEARNING STRATEGY:

Following are some sample strategies that can be incorporate for the Course Delivery

- Chalk and Talk Method/Blended Mode Method
- Power Point Presentation
- Expert Talk/Webinar/Seminar
- Video Streaming/Self-Study/Simulations
- Peer-to-Peer Activities
- Activity/Problem Based Learning
- Case Studies
- MOOC/NPTEL Courses
- Any other innovative initiatives with respect to the Course contents

LIST OF EXPERIMENTS

Sl. No.	Description
1	Demonstrate Network Packet analysis using WireShark tool.
2	Demonstrate Web penetration testing using BURP Suite tool.
3	Show Network mapping and port scanning using Nmap tool.
4	Implement a code to simulate buffer overflow attack. Code implementation can be written in any langauge
5	Demonstrate any of Cryptographic algorithm using JCryp tool.
6	Demonstrate Network reconnaissance using WHOIS tool.
7	Show how to detect ARP Spoofing using open-source tool ARPWATCH.
8	Demonstrate network vulnerabilities by scanning network using Nessus tool
9	Demonstrate network testbed Emulab.
10	Study of Information Technology Act, 2000 (India)

COURSE OUTCOMES

Upon completion of this course, the students will be able to:

CO No.	Course Outcome Description	Bloom's Taxonomy Level
CO1	Experiment with network packet analysis using the different pentesting tools	CL3
CO2	Classify network vulnerabilities, identify potential threats, and develop effective strategies for securing network infrastructure.	CL4
CO3	Distinguish different cryptographic algorithms and their capabilities	CL4
CO4	Classify ARP Spoofing using open-source tools	CL4
CO5	inspect and demonstrate network vulnerabilities effectively	CL4

CO-PO-PSO MAPPING

CO No.	Programme Outcomes (PO)												Programme Specific Outcome (PSO)		
	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3
CO1	3	3	3	1	3	2		1	3	2	2	3	3	3	3
CO2	3	3	3	1	3	2		1	3	2	2	3	3	3	3
CO3	3	3	3	1	3	2		1	3	2	2	3	3	3	3
CO4	3	3	3	1	3	2		1	3	2	2	3	3	3	3
CO5	3	3	3	1	3	2		1	3	2	2	3	3	3	3

3: Substantial (High) | **2: Moderate (Medium)** | **1: Poor (Low)**

ASSESSMENT STRATEGY

Assessment will be both CIA and SEE. Students learning will be assessed using Direct and Indirect methods:

Sl. No.	Assessment Description	Weightage (%)	Max. Marks
1	**Continuous Internal Assessment (CIA)**	**100 %**	**50**
	Laboratory Work (A)	50 %	25
	Laboratory Test (B)	30 %	15
	Open Ended Experiments /Mini Projects (C)	20 %	10
2	**Semester End Examination (SEE)**	**100 %**	**50**

ASSESSMENT STRATEGY:

I. In Laboratory Courses where (B) and (C) are not the components of the assessment pattern, then (A) will have 100% weightage (50 Marks).

Assessment Mode: Weekly Assessment of Laboratory Work (50 Marks) - the marks will be awarded based on the Continuous Internal Assessment (Weekly Assessment, each of 25 marks) of the students in each laboratory session. The average of all the marks obtained across the sessions will be the Final CIA marks.

II. In Laboratory Courses where (C) is not a component of the assessment pattern, then (A) will have 50% weightage (25 Marks), and (B) will have 50% weightage (25 Marks).

Assessment Mode: The marks will be awarded based on the Continuous Internal Assessment (Weekly Assessment) (A) and One Laboratory Test (B).

- In Weekly Assessment, the student will be evaluated in each laboratory session for 25 marks. The average marks obtained across all the experiments will be the marks obtained for (A).
- A Laboratory Test, similar to the SEE exam is conducted towards the end of the Semester/Course, whichever is earlier. The obtained marks are scaled down to 25 Marks (B)

The Sum of marks obtained across (A) and (B) will be the Final CIA marks.

III. In Laboratory Courses where (C) is a component of the assessment pattern, then assessment will be done by considering the weightages given above, i.e. (A) – 25 Marks (Weekly Assessment), (B) – 15 Marks (Laboratory Examination), (C) – 10 marks (Open Ended Experiments/Mini Projects)

- The respective course instructor will design the assessment criteria for the said assessment components.
- The assessment components will be made known to the students by the respective Course Coordinators prior to the commencement of the Laboratory Work.
- In all the cases, the assessments will be done based on the criteria designed by the Course Coordinator.

SEE QUESTION PAPER PATTERN:

1. All laboratory experiments should be included for practical examination, from which students are allowed to pick one experiment from the lot.
2. SEE shall be conducted for 100 Marks and the marks will be scaled down to 50.
3. General Marks Distribution: Procedure + Conduction + Viva = 20% + 50% + 30%.
4. Change of experiment is allowed only once and 20% of the marks allotted to the Procedure will be made ZERO (if a question carries two experiments, both should be changed). The evaluation will be done for 80% of the total maximum marks.