Shah & Anchor Kutchhi Engineering College

CURRICULUM STRUCTURE SECOND YEAR B.Voc.



Shah & Anchor Kutchhi Engineering College

Programme Curriculum for Bachelor of Engineering
Effective from
(with effect from academic year 2021-2022)

Semester III

Course Code	Name of the Course	Scheme of Instruction: Hours per Week		Scheme of Instruction: Total Credits	Scheme of Examination: Duration in Hours	Scheme of Examination: Maximum Marks				Total marks
		L	T			MSE	CIA	Total	ESE	
	Fundamentals of Computing Systems	3		3			30	30		30
	Data Structures	3		3	3	30	30	30	60	120
	Computer Network	3		3	3	30	30	30	60	120
	Audit Course						Grade		Grade	
	Kannada Kalpataru (Foundational Level)		2	0			30			30
	Environmental Data Analysis Lab		2	1	3		30		70	100
	Communication Skill-Advanced Lab		2	1	3		30		70	100
	Java Fundamentals: A Hands-On Approach		4	2	3		30		70	100
	OE1/PE1/HS1/P (Choose one from each) 1. Introduction to Energy Engineering and Applications 2. Art: Museum Analysis 3. Positive Psychology 4. IT: Research analysis 5. Self Software Analysis 6. Any Course using MOOC Level 5 or MOOC level 6			03			150			150
Total		9	10	16			270		330	600

Note: Note: (Theory/Practical) will be conducted for 100 marks and converted according to the appropriate weightage and considered as follows.
CIA: Continuous Internal Assessment ESE: End Semester Exam
MSE: Mid Semester Exam
OEP: Open Elective/Professional Elective HS: Humanities/Social Sciences and Management

Shah & Anchor Kutchhi Engineering College

Programme Structure for Second Year (B.Tech. in
Cyber Security
(with effect from academic year

Semester IV

Course Code	Name of the Course	Scheme of Instruction			Scheme of Examination					
		Hours per Week		Total Credits	Duration in Hours	Maximum Marks				Total marks
		L	T			ESE	CIE	Viva	TW	
	Physics	3		3			30	20		50
	Artificial Intelligence & Machine Learning in Security	3		3	2	70	20	10	50	150
	Fundamentals of Internet Architecture	3		3	2	70	20	10	50	150
	Skill Development									
	Programming with Python Lab		2	1	2		30		50	100
	Security of Embedded Lab		2	1	2		30		50	100
	Cybersecurity Investigations Lab		2	1			30			30
	Internship/Industry Training		2	1			30			30
	[illegible] 1. Computer Based Communication Networks and Architecture. [illegible] 2. Cloud Infrastructure Practice. [illegible] 3. Web Practice. [illegible] 4. Product Manager - Web & Mobile. [illegible] 5. Application Architect - Web & Mobile. [illegible] 6. Full Stack with MEAN Stack.			11			100			100
Total		09	04	13			310		200	510

Note: [illegible] will be conducted for 100 marks and converted according to the approved rule binding and practicals scheme.
CIE - Continuous Internal Examination; TW - Practical/Oral Examination; ESE - End Semester Examination.

Program:	Second Year B.Tech. (Semester III)	L	P	C
Fundamentals of Operating System	Course Code: BWCS0IC0301	3	-	3
Systems Architecture Practical	Lab Code: BWCS0IL0302	-	4	2
		3	4	5

Course Objective No.	Objective Description
1	To learn how operating systems work and how different types of OS and kernels are structured.
2	To use different methods for managing processes, threads, and solving synchronization and deadlock problems.
3	To apply memory management techniques like paging, segmentation, and page replacement.
4	To explore how file systems, I/O devices, and OS-level security features work.

CO No.	Course Outcome Description
CO1	Describe the basic functions of an operating system and compare different OS structures and kernels.
CO2	Implement process scheduling algorithms and analyze synchronization problems using semaphores and inter-process communication.
CO3	Apply memory allocation and page replacement techniques using suitable algorithms.
CO4	Demonstrate file organization, access control, and I/O scheduling techniques used in operating systems.

Pre-requisite courses: Basic Programming Skills of C.

DIRECT Assessment
1. Continuous Internal Assessment (Theory component)
2. Assignments / Tutorials / Power point presentation / Group discussion / Quiz / Seminar / Case studies / Design Thinking / Innovation / Creativity (Blog writing / Viogging, etc.)
3. Pre/Post - Experiment Test / Viva / Experimental Write-Up for each Experiment, Day to Day Experiments / Assignments / Tutorials / Power point presentation / Group discussion / Quiz / Seminar / Case studies / Design Thinking / Innovation / Creativity (Blog writing / Viogging, etc.) (Lab Component)
4. End Semester Examination (Theory and Lab component)
INDIRECT Assessment
1. Questionnaire survey
2. Activity based survey (if any)

Detailed Syllabus

Module	Hours	Course Outcome
Module 1: Basics of Operating Systems	8h	CO1
1.1 Introduction, Objectives of Operating System 1.2 Functions and Evolution of Operating System - Different Types of OS 1.3 Types of System Structures: Layered, Monolithic, and Microkernel 1.4 Concepts Related: Shell, and System Calls		
Module 2: Process Management	12	CO2
2.1 Process Management: Process concept, State Transition diagram, Process control block, Types of scheduler 2.2 Process Scheduling: Preemptive, Non preemptive, CPU scheduling algorithms: FCFS, SJF, RR, Priority, MLFQ, Context switch, Threading, Multithreading model 2.3 Process cooperation and synchronization: Concurrency problems, Critical section problem, Semaphores, Conditional critical regions, Classical inter-process Communication Problems: Dining Philosophers Problem, Producer and Consumer Problem. 2.4 Deadlock:System Model, Deadlock characterization, Deadlock Prevention, Deadlock Avoidance, Deadlock Detection and Recovery		
Self learning: Process Management in multicores OS		
Module 3: Memory Management	08	CO3
3.1 Basics of Memory Management and Pixel Performance 3.2 Dynamic Partitioning and Memory Allocation Methods: First Fit, Best Fit, Worst Fit 3.3 Memory Management Techniques: Paging, Segmentation, and Use of TLB 3.4 Demand Paging, Page Replacement Strategies (FIFO, Optimal, LRU)		
Module 4: File Systems & I/O Management	08	CO4
4.1 Overview, File Organization and Access, File Directories, File Sharing, File Security, File structure and Access Control Methods 4.2 I/O devices, Organization of the I/O Functions, Disk Organization 4.3 I/O Management and Disk Scheduling: FCFS, SSTF, SCAN, CSCAN, LOOK, C-LOOK.		

Lecture: 2 Hrs/Week	Total Hours: 36

Lab Component:

Suggested List of experiments (Any 10 Experiments out of the given list)

S.No.	Experiment Title	Course Outcomes
1	Install and configure a Linux Operating System	CO1
2	Introduction to Linux Shell Commands and File Operations	CO1
3	Create and Execute a Simple C Program using Linux Terminal	CO1
4	Program to Create a Child Process using fork()	CO1
5	Implement FCFS Scheduling Algorithm in C	CO2
6	Implement SJF Scheduling Algorithm in C	CO2
7	Implement Round Robin Scheduling Algorithm in C	CO2
8	Configure Guest user Policies using Groupware (Simple Version)	CO2
9	Simulate First Fit Memory Allocation using Arrays in C	CO3
10	Simulate Best Fit Memory Allocation using Arrays in C	CO3
11	Simulate FIFO Page Replacement Algorithm	CO3
12	Simulate LRU Page Replacement Algorithm	CO3
13	Explore Web Penetration using nikto and w3 Commands	CO4
14	Create and Read a File using fopen() and fread() in C	CO4
15	Simulate FCFS Disk Scheduling Algorithm	CO4
16	Simulate SCAN Disk Scheduling Algorithm	CO4

Practicals: 4 Hrs/Week	Total Hours: 60

Text Books

Sr. No	Title	Edition	Authors	Publisher	Year
1	Operating systems: internals and design principles	7th Edition	Stallings, William	Prentice Hall Press	2011
2	Operating System Concepts	9th Edition	Abraham Silberschatz, Peter Baer Galvin and Greg Gagne & John Wiley	Sons, Inc.	2016

Reference Books

Sr. No	Title	Edition	Authors	Publisher	Year
1	Operating System Design and Implementation	3rd Edition	Andrew Tanenbaum	Pearson	2006
2	Operating Systems	8th Edition	Achyut Godbole and Atul Kahate	McGraw Hill Education	2010

Online References

Sr. No	Website Name
1	https://vlabs.iitb.ac.in/vlab/
2	https://nptel.ac.in/courses/106/105/106105214/

Program	Second Year B. Tech. (Semester III)	L	P	C
Data Structures	Course Code: BVCSBSC20C23	3	-	3
Structured Data Analysis Lab	Lab Code: BVCSBSC20L22	-	2	1
		3	2	4

Course Objective No.	Objective Description
1	To understand the need and significance of Data structure as a computer Science mind.
2	To analyze various data structures and select the appropriate one to solve a specific real-world problem.
3	To introduce various techniques for representation of the data in the real world.
4	To teach concepts of Linear and Nonlinear data structures also learn understanding techniques.

CO No.	Course Outcome Description
CO1	Explain Linear and Non-Linear data structures and list types and able to handle various operations on data structure like stack , queue with its applications.
CO2	Analyze various operations on Linked lists like searching, insertion, deletion and traversals.
CO3	Explain key related terminologies and list types as well as operations on various tree type data structures.
CO4	Demonstrate graph related terminologies and its traversing technique as well as operations on Graph type data structure.

Pre-requisite courses: C Programming (Loops, Structures and Pointers)

DIRECT Assessment
1. Continuous Internal Assessment (Theory component) 2. Assignments / Tutorials / Power point presentations / Group discussion / Quiz / Seminar / Case studies / Design Thinking / Innovation / Creativity (Blog writing / Viogging, etc.) 3. Practical – Experiment Title / Aim / Experimental Setup for each Experiment, Day to Day Experiments / Assignments / Tutorials / Power point presentation / Group discussion / Quiz / Seminar / Case studies / Design Thinking / Innovation / Creativity (Blog writing / Viogging, etc.) (Lab Component) 4. End Semester Examination (Theory and Lab component)
INDIRECT Assessment
1. Course exit survey 2. Activity based survey (Expert)

Detailed Syllabus

Module	Hours	Course Outcome
Module 1: Introduction to Data Structures, Stack and Queues	15	CO1
1.1 Introduction to Data Structures, Concept of ADT, Types of Data Structures Linear and Nonlinear, Operations on Data Structures 1.2 Stack: Introduction, ADT of Stack, Operations on Stack, Array Implementation of Stack, Applications of Stack: Well Formedness of Parenthesis, Infix to Postfix Conversion and Postfix Evaluation, Recursion. 1.3 Queue: Introduction, ADT of Queue, Operations on Queue, Array Implementation of Queue, Types of Queue: Circular Queue, Priority Queue, Introduction to Double Ended Queue. 1.4 Using Stack and Queue to Simulate a Personal Safe Checker		
Module 2: Linked List	10	CO2
2.1 Introduction, Representation of Linked List, Linked List v/s Array 2.2 Types of Linked List - Singly Linked List, Circular Linked List, Doubly Linked List. 2.3 Operations on Singly Linked List and Doubly Linked List, Stack and Queue using Singly Linked List, Singly Linked List		
Module 3: Trees	12	CO3
3.1 Introduction, Tree Terminologies, Binary Tree, Binary Tree Representations 3.2 Types of Binary Tree, Binary Tree Traversals, Binary Search Tree. 3.3 Operations on Binary Search Tree, Applications of Binary Tree-Expression Tree. 3.4 Huffman Encoding, Search Trees (ST), rotations in AVL Tree, operations on AVL Tree.		
Module 4: Graphs & Searching, Hashing	9	CO4
4.1 Introduction, Graph Terminologies, Representations of Graph 4.2 Graph Traversals: Depth First Search (DFS) and Breadth First Search (BFS). 4.3 Linear Search algorithm, Binary Search algorithm		

Lectures: 3 Hrs/Week	Total Hours: 46

Lab Component:

Suggested List of experiments (Any 8 Experiments out of the given list)

S.No.	Experiment Title	Course Outcomes
1	Implement Stack ADT using an array	CO1
2	Convert an Infix expression to Postfix expression using stack ADT	CO3
3	Evaluate Postfix Expression using Stack ADT	CO3
4	Applications of Stack ADT	CO3
5	Implement Linear Queue ADT using an array	CO3
6	Implement Circular Queue ADT using an array	CO3
7	Implement Priority Queue ADT using an array	CO3
8	Implement Singly (Linked) List ADT	CO2
9	Implement Circular Linked List ADT	CO2
10	Implement Doubly Linked List ADT	CO2
11	Implement Stack / Linear Queue ADT using Linked List	CO2
12	Implement Binary Search Tree ADT using Linked List	CO3
13	Implement Graph Traversal techniques: a) Depth First Search b) Breadth First Search	CO5
14	Applications of Binary Search Technique	CO4

Labs: 2 Hrs/Week	Total Hours: 30

Text Books

Sr. No	Title	Edition	Authors	Publisher	Year
1	Data Structures using C	2nd Edition	Reema Thareja	Oxford Press	2014
2	Data Structures Using C	2nd Edition	Aaron M Tenenbaum, Yedidyah Langsam, Moshe J Augenstein	Prentice Hall of India	2009
3	Data Structures: A Pseudocode Approach with C	2nd Edition	Richard F. Gilberg and Behrouz A. Forouzan	Course Technology	2005
4	Data Structures Using C	2nd Edition	ISRD Group	Tata McGraw Hill	2006

Reference Books

Sr. No	Title	Edition	Authors	Publisher	Year
1	[illegible]	2nd Edition	Mark Allen Weiss	Pearson	2013
2	Algorithms	4th Edition	Robert Sedgewick and Kevin Wayne	Pearson	2011
3	[illegible]	3rd Edition	Adam Drozdek	[illegible]	2005
4	Introduction to Algorithms	3rd Edition	Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein	MIT Press	2009

Online References

Sr. No	Website Name
1	[illegible]
2	[illegible]

Program	Second Year B.Tech. (Semester III)	L	P	C
Computer Network	Course Code: BTCSBSC20C23	3	-	3
Communication Networks Lab	Lab Code: BTCSBSC20P23	-	2	1
		3	2	4

Course Objective No.	Objective Description
1	To understand the fundamental concepts of networking standards, protocols and technologies.
2	To learn different techniques for framing, error control, flow control and routing.
3	Explain transport and application layer protocols for reliable network communication.
4	To describe network layouts, WAN technologies, and tools used for secure and efficient network operations.

CO No.	Course Outcome Description
CO1	Summarize fundamental concepts of Computer Networks, architectures, protocols and technologies.
CO2	Apply data link layer functions and analyze various routing protocols and mechanisms.
CO3	Apply transport services and protocols for human communication and other application-layer protocols for network communication.
CO4	Apply security measures and tools to diagnose and troubleshoot network issues.

Pre-requisite courses: Basic understanding of computer hardware and operating systems.

DIRECT Assessment
1. Continuous Internal Assessment (Theory component) 2. Assignments / Tutorials / Power point presentations / Group discussion / Quiz / Seminar / Case studies / Design Thinking / Interviews / Creativity (Blog writing / Viogging, etc.) 3. Practical – Experiment Viva / Vivo / Experimental Write-Up for each Experiment, Day to Day Experiments / Assignments / Tutorials / Power point presentations / Group discussion / Quiz / Seminar / Case studies / Design Thinking / Interviews / Creativity (Blog writing / Viogging, etc.) (Lab Component) 4. End Semester Examination (Theory and Lab component)
INDIRECT Assessment
1. Course end survey 2. Alumni/Employer survey (if any)

Detailed Syllabus

Module	Hours	Course Outcome
Module 1: Fundamentals of Computer Networking	10	CO1
1.1 Introduction to Computer Networks: Common Network Components (LAN, MAN, WAN, VPNs) Physical Network Topologies (Bus, Star, Ring, Mesh, Point to Point, Point to Multipoint, Hybrid) 1.2 Devices and services at their appropriate OSI reference model and TCP/IP model. 1.3 Purpose and uses of ports and protocols at each layer of OSI reference Model, comparison of OSI and TCP/IP reference model. 1.4 Introduction to Network Devices: Hub, Switch, Router, Modem, Access Point, Media types: Copper, UTP, STP, Coaxial, Fiber, Implementation		
Module 2: Switching and Routing Concepts	11	CO2
2.1 Introduction to Data link Layer: OSI Design Issue (Services, Framing, Error Control, Flow Control) 2.2 Detection and Correction (Hamming Code, CRC, Checksum), Elementary Data Link protocols, Stop and Wait, Sliding Window (Go Back N, Selective Repeat). 2.3 Purpose of IP addresses, Structure of IPv4 address (32 bit), Binary and decimal conversion (IPv4 Addressing (classful and classless), Subnetting, IPv4 Protocol, Introduction to IPv6 addressing, IPv6 Address Representation & Compression.		
Module 3: Higher Layer Protocols	12	CO3
3.1 The Transport Service: Transport service primitives, Berkeley Sockets, Elements transport (Handshake), UDP, TCP, TCP state transition, TCP (based TCP Flow control (Sliding Window), TCP Congestion Control. 3.2 Application Layer Protocol: DNS: Name Space, Resource Record and Types of Name Server, HTTP (Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol), DHCP (Dynamic Host Configuration Protocol), Remote access methods: Telnet, FTP, SFTP.		
Module 4: Network Security, WAN Protocols, and Troubleshooting Tools	12	CO4
4.1 Network Threats and Mitigation: Recognizing Security Threats, Defining Firewall, Firewall Technologies, Intrusion Detection and Prevention Systems. 4.2 Wide Area Networks: WAN Protocols, Command Line Tools (Ipconfig, ping, tracert, nslookup, netstat, ARP, nslookup, Nbtstat, Net and Route Command, telnet Utility, FTP, Telnet Utility) 4.3 Software and Hardware Tools: Network Scanners, Identifying Hardware Tools, Network Troubleshooting, Troubleshooting Steps and Tips, Monitoring and Optimization.		

Lectures: 3 Hrs/Week	Total Hours: 45

Lab Component:

Suggested list of experiments (Point the given list of topics, prepare any 12 case study on scenario-based experiments like the one shown in Experiment 8).

S.No.	Experiment Title	Course Outcomes
1	Introduction to Network Simulation Software (e.g., Cisco Packet Tracer)	CO1
2	To design and implement different physical network topologies (Bus, Star, Ring, Mesh) using a simulation tool (e.g., Cisco Packet Tracer or GNS3). For E.g. Case Study/Scenario: You have been tasked with designing and implementing five different physical network topologies (Bus, Star, Ring, and Mesh) for a growing organization using a simulation tool like Cisco Packet Tracer or GNS3. Each topology must be configured with multiple devices, tested for connectivity, and analyzed for performance, scalability, and reliability. The goal is to evaluate the strengths and weaknesses of each topology and recommend the most suitable design for the organization's expanding network needs.	CO1
3	To understand encapsulation and OSI layers using Wireshark.	CO1
4	To identify and create different network cables: straight-through, crossover, and rollover. (Crimping tool, RJ-45 connectors, cable tester)	CO1
5	To analyze Ethernet frames and MAC addressing.	CO2
6	To practice IP addressing, subnetting, and address classification (e.g., Cisco Packet Tracer).	CO3
7	To configure static and dynamic routing between networks. (e.g., Cisco Packet Tracer)	CO3
8	To create VLANs and configure inter-VLAN communication.	CO3
9	To configure Network Address Translation and troubleshoot IP issues.	CO3
10	Demonstrate the encapsulation process and transmit packet headers using a real-world protocol analyzer. (Use Wireshark to capture ICMP packets and analyze the layers of TCP/IP.)	CO2
11	To secure a network using Access Control Lists and simulate a basic firewall.	CO3
12	Use Packet Tracer to configure OSPF on one topology and EIGRP on another.	CO3
13	To configure WAN links and use basic network diagnostic tools.	CO4
14	To create, monitor, and optimize network performance (SNMP Tool).	CO4
15	Create and manage local user accounts and enforce password policies in Windows/Linux, and Configure firewalls and antivirus in a Linux environment (MIT Professor).	CO5

Lab: 4 Hrs/Week	Total Hours: 60

Text Books

Sr. No	Title	Edition	Authors	Publisher	Year
1	Computer Networks	4th Edition	ANDREW S. TANENBAUM	Pearson Education	2003
2	Data Communications and Networking	2nd Edition	B.A. Forouzan	TMH	2003
3	Computer Network, 5e: A Top-Down Approach Featuring the Internet	4th Edition	James F. Kurose, Keith W. Ross	Addison Wesley	2009
4	Computer Networks	5th Edition	ANDREW S. TANENBAUM	Pearson	2011

Reference Books

Sr. No	Title	Edition	Authors	Publisher	Year
1	Interconnecting with [illegible], Vol. 1 (Subnetting, Protocols, and Architecture)	4th Edition	Mark Allen Weiss	Pearson	2013
2	[illegible] Protocol Suite	4th Edition	Behrouz A. Forouzan	The McGraw-Hill	2010
3	Data communication and Networking	4th Edition	Behrouz A. Forouzan	The McGraw-Hill	2007

Online References

Sr. No	Website Name
1	https://www.coursera.org/[illegible]
2	https://[illegible]

Program:	Second Year B.Tech. (Semester III)	L	P	C
Java Programming & Web Based Application	Course Code: BWSBSMEV211		4	2

Course Objective No.	Objective Description
1	To introduce the principles of Object Oriented Programming (OOP) and basic Java syntax.
2	To develop understanding of Java class structures, input/output, and package management.
3	To apply concepts of inheritance, exception handling, and multithreading for robust software development.
4	To enable students to design Graphical User Interfaces (GUI) using AWT and Swing for interactive Java applications.

CO No.	Course Outcome Description
CO1	Apply the basic principles of object-oriented programming and implement simple programs using Java syntax, arrays, and strings.
CO2	Implement modular programs using classes, objects, constructors, method overloading, packages, and input/output techniques.
CO3	Apply advanced Java concepts like inheritance, interfaces, exception handling, and multithreading to build efficient and error-resistant programs.
CO4	Implement GUI applications using Java applets, AWT components, event handling, and Swing for enhanced user interaction.

Pre-requisite courses: Basic computer literacy and problem-solving skills.

DIRECT Assessment
1. Continuous External Assessment (Theory component) 2. Assignments / Tutorials / Power point presentation / Group discussion / Quiz / Seminar / Case studies / Design Thinking / Innovation / Creativity (Blog writing / Viva voce, etc.) 3. Pre/Post / Experiment Test / Viva / Experimental Skills (To be each Experiment) Day to Day Experiments / Assignments / Tutorials / Power point presentation / Group discussion / Quiz / Seminar / Case studies / Design Thinking / Innovation / Creativity (Blog writing / Viva voce, etc.) (Lab Component) 4. End Semester Examination (Theory and Lab components)
INDIRECT Assessment
1. Course end survey 2. Activity based survey (if any)

Detailed Syllabus

Module	Hours	Course Outcome
Module 1 Introduction to Object Oriented Programming and Java	15	CO1

1.1. OOP Concepts: Objects, Class, Encapsulation, Abstraction, Inheritance, Polymorphism, Message Passing.

1.2. Java Virtual Machine: Overview of JVM and its role in Java execution.

1.3. Basic Programming Constructs: Variables, Data Types, Operators, Expressions, Branching and Looping.

1.4. Arrays: Declaration, Initialization and Usage in Java.

1.5. Strings and StringBuffer Classes.

Module 2 Classes, Objects, Packages and I/O Handling	15	CO2

2.1. Class, Object, Data Members, Member Functions.

2.2. Constructors and Types: Parameterized, Default, and Copy Constructors.

2.3. Static Members and Functions.

2.4. Method Overloading.

2.5. Packages: Types of Packages, Built-in and user-defined packages.

2.6. Input and Output Functions: Reading from and writing to console and files.

2.7. Wrapper classes: Class, Scanner Class.

Module 3: Inheritance, Interfaces, and Exception Handling	15	CO3

3.1. Types of Inheritance, Method Overriding, super.

3.2. Abstract Class and Method.

3.3. final Keyword, extends Keyword.

3.4. Multiple Inheritance using Interface.

3.5. try, catch, throw, throws, User-defined Exceptions.

3.6. Thread Lifecycle, Thread Class Methods, Creating Threads: extends, implements.

Module 4: GUI Programming in Java	15	CO4

4.1. Applet Life Cycle, Creating Applets.

4.2. Graphics Class Functions.

4.3. Parameter Passing to Applet.

4.4. Font and Color Class.

4.5. Event Handling using Event Classes.

4.6. AWT: Windows and GUI Controls.

4.7. Introduction to Swing in Java.

Practical: 1Hrs/Week	Total Hours: 60

Lab Component:

Suggested List of experiments (Any 10 Experiments out of the given list)

S.No.	Experiment Title	Program Outcomes
1	Programs on basic programming constructs like branching and looping	PO1
2	Program on accepting input through keyboard	PO1
3	Program on class and objects	PO2
4	Program on method and constructor overloading	PO3
5	Program on Packages	PO3
6	Program on 2D array using functions	PO3
7	Program on Strings class and Methods	PO3
8	Program on types of Inheritance	PO3
9	Program on Multiple Inheritance	PO3
10	Program on abstract class and abstract methods	PO3
11	Program using upper and lower bounds	PO3
12	Program on Exception handling	PO3
13	Program on user-defined exception	PO3
14	Program on Multithreading	PO3
15	Program on Applet class	PO3
16	Program on Applet class	PO3
17	Program to create GUI applications	PO3
18	Mini Project based on the content of the syllabus (Group of 2-3 students)	PO3, PO5

Text Books

Sr. No	Title	Edition	Authors	Publisher	Year
1	Java: The Complete Reference by Herbert Schildt An extensive guide covering Java language features, libraries, and best practices	9th Edition	Herbert Schildt	Tata McGraw-Hill	2014
2	Programming with Java	4th Edition	E. Balagurusamy	McGraw Hill Education	2019
3	Java Programming	9th Edition	Joyce Farrell	Cengage	2018

Reference Books

Sr. No	Title	Edition	Authors	Publisher	Year
1	Beginning JAVA	8th Edition	Ivor Horton	Wiley India	2009
2	Java: How to Program	8th Edition	Deitel and Deitel	PHI	1998
3	JAVA Programming	1st Edition	Black Book	Dreamtech Press	2011
4	Learn to Master Java programming	1st Edition	script Orange	Harish solutions	-

Online References

Sr. No	Website Name
A	https://www.coursera.org/learn/advanced-concepts-of-object-oriented-programming
B	www.edureka.co.com
C	www.tutorialspoint.com
D	https://nptel.ac.in/courses/106105191/javaclass
E	https://www.coursera.org/learn/java-concepts-1

Program:	Second Year B.Tech. (Semester III)	L	T	C
UIT/NME/QP (Choose Any One) 1. Certificate Program in Prompt Engineering and ChatGPT (NE101, NE102, NE103, NE104, NE105) 2. Security Analyst (SOC) (QE001) 3. Security Operations Center Analyst (SOC) (QE002) 4. Application Security Analyst (SOC) (QE003) 5. Any Other with NSQF Level 5 or NSQF Level 5.5	Choose Codes: [illegible]	-	-	03

Sr. No.	UIT/NME/QP (Choose Any One)	Syllabus for the qualifier Pack is available on:
1.	Certificate Program in Prompt Engineering and ChatGPT (NE101, NE102, NE103, NE104, NE105)	[illegible] Qualification Pack
2.	SOC Analyst (SOC) (QE001)	[illegible] Qualification Pack
3.	Security Operations Center Analyst (SOC) (QE002)	[illegible] Qualification Pack
4.	IT Forensic Analyst (SOC) (QE003)	[illegible] Qualification Pack
5.	SOC Delivery Analyst (SOC) (QE004)	[illegible] Qualification Pack
6.	Any Other with NSQF Level 5 or NSQF Level 5.5	

Program:	Second Year B. Tech. (Semester IV)	L	P	C
Python	Course Code: BWSBSC0304	1	-	1
Programming with Python Lab	Lab Code: BWCSBSE0341	-	4	2
		1	4	3

Course Objective No.	Objective Description
1	To introduce students to Python programming concepts, data types, control structures, functions, object-oriented programming, and foundational data structures.
2	To enable students to develop GUI applications, implement database connectivity, and understand multithreading concepts in Python.
3	To introduce web development concepts using HTML, CSS, and Django framework for dynamic web applications.
4	To provide practical knowledge of data manipulation and analysis using NumPy arrays and Pandas data structures.

CO No.	Course Outcome Description
CO1	Write efficient Python programs using functions, OOP, and basic data structures like lists, tuples, and sets.
CO2	Develop interactive applications with GUI interfaces, manage data using databases, and implement multithreaded processes.
CO3	Design and develop basic web applications using Django, incorporating forms, templates, and styling.
CO4	Create, manipulate, and analyze structured datasets using NumPy and Pandas for real-world applications.

Pre-requisite courses: Computer Science Fundamentals, Data Structures and Algorithms

DIRECT Assessment
1. Continuous Internal Assessment (Theory component) 2. Assignments / Tutorials / Power point presentation / Group discussion / Quiz / Seminar / Case studies / Design Thinking / Innovation / Creativity (Blog writing / Vlogging, etc.) 3. Pre/Post - Experiment Test / Viva / Experimental Write-Up for each Experiment, Day to Day Experiments / Assignments / Tutorials / Power point presentations / Group discussion / Quiz / Seminar / Case studies / Design Thinking / Innovation / Creativity (Blog writing / Vlogging, etc.) (Lab Component) 4. End Semester Examination (Theory and Lab components)
INDIRECT Assessment
1. Questionnaire survey 2. Activity based survey (if any)

Detailed Syllabus

Module	Hours	Course Outcomes
Module 1: Python Essentials	10	CO1
1.1 Introduction to Python, Basic Syntax and Data Types (variables, Data Types: int, float, string, list, tuple, dictionary, set), Operators and Expressions, Control Flow and Loops 1.2 Functions and Modules – Defining and Calling Functions, Function Arguments, Lambda Functions, Modules and Packages, Exception Handling – Try-Except Blocks, Raising Exceptions 1.3 Object-Oriented Programming – Classes and Objects, Constructors, Inheritance, and Polymorphism. 1.4 Data Structures in Python: Linked List, Stack, Queue, Dequeue.		
Self Learning: Input validation and sanitization, Use of exception handling to prevent software from crashes		
Module 2: Advanced Python: DBMS, Databases, and Concurrency	07	CO2
2.1 Introduction to GUI Programming – GUI Frameworks (Tkinter) (Tkinter Pdf) 2.2 Introduction to Database Connectivity in Python, Connecting Python to Database 2.3 Multithreading: Thread and Process, creating a thread, threading module, Synchronizing threads, Multithreaded Priority Queue.		
Self Learning: Handling resource leaks and dynamic code execution, Protecting sensitive data in GUI (e.g., passwords)		
Module 3: Web Dev with Django	08	CO3
3.1 Introduction to Django Framework, Django URLs and Views, Understanding Django URL Dispatcher, Creating URL patterns, Creating Views using Functions and Class-Based Views, Passing Data from Views to Templates via Context 3.2 Django Templates – Template Structure and Location, Using render() to load Templates, Django Template Language (DTL), Django Difference Between HTML Forms and Django Forms, Creating Forms, Rendering Forms in Templates, Validating User Input with Django Form Validation, Displaying Form Errors in Templates 3.3 Web page consolidation tools (HTML and CSS).		
Module 4: Data Handling with NumPy & Pandas	08	CO4
4.1 NumPy: Creating NumPy arrays and multidimensional arrays, NumPy's Data types, Array Attributes, Indexing and Slicing, reading array from/to files, Manipulating array shapes (2D) 4.2 Pandas: Basics of Pandas, Using multidimensional series, Series and Data Frames, Grouping, aggregating, Merge Data Frames.		
Self Learning: Detecting unauthorized changes in datasets, Encryption and password protection		

Lectures: 2 Hrs/Week	Total Hours: 39

Lab Component:

Suggested List of experiments (Any 10 Experiments out of the given list)

S.No.	Experiment Title	Course Outcomes
1	Write a Python program to demonstrate data types, variables, and type casting.	CO1
2	Implement conditional statements and loops to build a small calculator.	CO1
3	Create and use user-defined functions with different argument types.	CO2
4	Develop a module with multiple functions and import it into another script.	CO2
5	Implement exception handling using try-except blocks with custom error messages.	CO2
6.	Create a class in Python demonstrating constructors, attributes, and methods.	CO3
7.	Develop an OOP example showing inheritance and method overriding.	CO3
8.	Implement stack and queue operations using Python lists.	CO3
9.	Design a simple GUI login window using Tkinter.	CO4
10.	Build a form-based GUI using tkTkinter with submit and reset buttons.	CO4
11.	Connect a Python application to MySQL and perform basic CRUD operations.	CO5
12.	Create a multithreaded Python program to simulate downloading multiple files.	CO5
13.	Build a basic Flask web app with a homepage and navigation through URLs.	CO5
14.	Design a Django template using HTML and CSS with form handling.	CO5
15.	Perform data manipulation using Pandas (merge, group, aggregate) on a CSV dataset.	CO6

Lab: 4 Hrs/Week	Total Hours: 60

Text Books

Sr. No	Title	Edition	Authors	Publisher	Year
1	Python for Everybody	1st Edition	Dr. Charles R. Severance	Shroff Publishers	2017
2	PROGRAMMING DATA MINING WITH PYTHON	1st Edition	Prof. Madhavan Mukund	NPTEL (National Programme on Technology Enhanced Learning)	2020
3	The Python Book	2nd Edition	Imagine Publishing	Imagine Publishing Ltd	2018

Reference Books

Sr. No	Title	Edition	Authors	Publisher	Year
1	Think Python How to Think Like a Computer Scientist	2nd Edition	Allen Downey	Green Tea Press	2015
2	Automate the Boring Stuff with Python Practical Programming	1st Edition	Al Sweigart	Nostrh Press	2015

Online References

Sr. No	Website Name
A	Judge: (Digital) on JavaScript(10010101)
B	Coursera "Python for Everybody Specialization"
C	Coursera "Google IT Automation with Python"

Program	Second Year B.Tech (Semester IV)	L	P	C
Artificial Intelligence and Machine Learning in Security	Lab Course: BYCS0000XXP22	0	4	4
Security AI Exploration Lab	Lab Course: BYCS0000XXP23	0	4	4
		0	8	8

Course Objective No.	Objective Description
1	To introduce how AI and machine learning are applied to cyber security.
2	To apply data preprocessing and feature engineering techniques to cyber security datasets for effective threat detection and analysis.
3	To provide practical exposure to applying machine learning models on real-world security datasets.
4	To study ethical implications and adversarial threats to AI systems in cyber security.

CO No.	Course Outcome Description
CO1	Describe the impact of AI/ML on cyber threats and defenses using case studies.
CO2	Apply data cleaning, normalization, and feature selection to cyber security data (like logs and network traffic) to improve machine learning model accuracy and threat detection.
CO3	Build and tune ML models for malware classification, anomaly detection, and other cybersecurity applications using appropriate evaluation metrics.
CO4	Analyze and discuss advanced AI-driven security solutions, including real-time threat detection, adversarial attacks, and ethical implications in cybersecurity.

Pre-requisite courses: Basic programming (Python preferred), linear algebra, statistics, and knowledge of cyber security concepts.

DIRECT Assessment
1. Continuous Internal Assessment (Theory components) 2. Assignments / Tutorials / Power point presentations / Group discussion / Quiz / Seminars / Case studies / Design Thinking / Innovation / Creativity (Blog writing / Viogging, etc.) 3. Pre/Post – Experiment Test / Viva / Experimental Work/Up for each Experiment, Due to the Experiments / Assignments / Tutorials / Power point presentations / Group discussion / Quiz / Seminars / Case studies / Design Thinking / Innovation / Creativity (Blog writing / Viogging, etc.) (Lab Components) 4. End Semester Examination (Theory and Lab components)
INDIRECT Assessment
1. Course end survey 2. Faculty feedback survey (if any)

Detailed Syllabus

Module	Hours	Course Outcome
Module 1: Python Essentials	15	CO1
1.1 Introduction to Artificial Intelligence: Definition, history, and relevance in cyber security 1.2 Types of AI: Symbolic AI, Machine Learning, Deep Learning, NLP 1.3 Machine Learning Paradigms: Supervised, Unsupervised, Semi-supervised, Reinforcement Learning 1.4 Overview of cyber security landscape: Threats, vulnerabilities, attack vectors 1.5 Role and impact of AI/ML in modern cyber security environments 1.6 Case studies: AI-driven cyber attacks and defenses 1.7 Ethical considerations and limitations 1.8 Use of exception handling to prevent vulnerability leakage		
Module 2: Data for Security Analytics	15	CO2
2.1 Importance of data quality in AI/ML models 2.2 Data sources in cyber security: System logs, network traffic, endpoint data 2.3 Data preprocessing: Cleaning, normalization, handling missing and imbalanced data 2.4 Feature engineering: Extraction and selection of relevant features for threat detection 2.5 Dealing with noisy and high-dimensional security data 2.6 Tools and platforms for data processing in security analytics 2.7 Assessing learner outputs and dynamic code execution 2.8 Protecting sensitive data in GCP (e.g., passwords)		
Module 3:ML Techniques for Threat Detection	10	CO3
3.1 Supervised learning for malware and intrusion detection: Algorithms and workflows 3.2 Unsupervised learning for anomaly and insider threat detection 3.3 Semi-supervised and reinforcement learning applications in cyber security 3.4 Model evaluation: Accuracy, Precision, Recall, F1 Score, ROC 3.5 Comparison: Supervised vs. Unsupervised learning for threat detection 3.6 Challenges in deploying ML models in real-world security environments 3.7 Adversarial Attacks and Defense Mechanisms: Types of adversarial attacks on AI models, Poisoning and evasion attacks in cybersecurity systems 3.8 Defense strategies: adversarial training, input preprocessing, robust models		

Module 6: Advanced Applications and Future Trends	15	CO6

6.1 AI in real-time threat detection and automated response (SOAR).

6.2 Adversarial machine learning: Attacks on AI models and defense strategies.

6.3 Deep learning for cyber security: Use cases and limitations.

6.4 AI for phishing, spam, and social engineering attack detection.

6.5 Security, privacy, and ethical considerations in AI/ML applications.

6.6 Current trends: Autonomous defense systems, explainable AI, and future research directions.

Lectures: 4 Hrs/Week	Total Hours: 60

Lab Component:

Suggested list of experiments (From the given List of topics, Prepare 10 Case Study /Scenario Based experiments like the one shown in Experiment 1

S.No.	Experiment Title	Course Outcomes
1	Spam Detection with Naive Bayes: Classify emails as spam/non-spam using a labeled dataset.	CO1
2	Anomaly Detection with K-Means Clustering: Identify outliers in network traffic data.	CO1
3	Reinforcement Learning for Firewall Rules: Simulate an RL agent optimizing firewall policies.	CO2
4	Cleaning Noisy Security Logs/Normalize Timestamps: Handle malformed entries, and export clean data.	CO2
5	Feature Extraction from Network Packets: Extract metadata (e.g., packet size, protocol) from PCAP files.	CO3
6	ML Techniques for Threat Detection: Train a model to classify malware families.	CO3
7	Intrusion Detection Using Random Forest: Detect network intrusions (for IDS) using scikit-learn.	CO3
8	ROC Curve Analysis for Phishing Detection: Plot ROC curves and evaluate AUC scores.	CO3
9	Adversarial Attack on a Classifier: Generate adversarial examples and test model robustness.	CO3
10	Phishing Detection with Neural Networks: Build a CNN to classify phishing web sites.	CO4
11	IP-Action information for SOC: Blocking, Quarantine, Control activities.	CO4
12	Case studies (e.g., IBM's AI Fusion SOC).	CO4

Lectures: 0 Hrs./Week	Total Hours:150

Text Books

Sr. No	Title	Edition	Authors	Publisher	Year
1	Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow	2nd Edition	Aurélien Géron	O'Reilly Media	2019
2	Deep Learning	1st Edition	Ian Goodfellow, Yoshua Bengio, and Aaron Courville	MIT Press	2016
3	Deep Learning: How does it ...A Visual, In-tuitive Guide to Artificial Intelligence	3rd Edition	Ian Kinsley, Chris Daybrook, Aglaé Bassens	Syllabus Books Pvt. Limited	2019

Reference Books

Sr. No	Title	Edition	Authors	Publisher	Year
1	Deep Learning with R	2nd Edition	JJ Allaire, Charles Tresser, Kalvinder, J.J. Allaire	Manning Publications	2020
2	Artificial Intelligence: A Guide for Thinking Humans	1st Edition	Melanie Mitchell	Farrar, Straus and Giroux	2019

Online References

Sr. No	Website Name
1	https://nptel.ac.in/courses/106/106/106106184/
2	https://www.coursera.org/learn/machine-learning
3	https://www.udacity.com/course/intro-to-machine-learning--ud120

Program	Second Year B.Tech (Semester IV)	L	P	C
Fundamentals of Ethical Hacking	Course Code: BWCS0402PC43	3	-	3
Cybersecurity Investigation Lab	Lab Code: BWCS0402PC43	-	3	1.5
		3	3	4.5

Course Objective No.	Objective Description
1	To understand fundamentals of ethical hacking
2	To learn advanced attacks like session hacking, malware, sniffing, social engineering, and SQL injection
3	To study network and web attacks like DoS, session hijacking, IDS evasion, and server hacking
4	To explore security risks and defenses in wireless, mobile, IoT, cloud computing, and cryptography

CO No.	Course Outcome Description
CO1	Perform footprinting, scanning, enumeration, and basic vulnerability assessments ethically
CO2	Detect and mitigate malware, session hacks, sniffing, social engineering, and SQL injections
CO3	Analyze and prevent network-based and web-based attacks using appropriate tools and techniques
CO4	Explore secure wireless, IoT, cloud, and cryptographic data with cybersecurity methods

Pre-requisite courses: Fundamentals of Cybersecurity

DIRECT Assessment
1. Continuous Internal Assessment [Theory component]
2. Assignments / Tutorials / Power point presentation / Quizzes/Seminars / Quiz / Seminar / Case studies / Design Thinking / Innovation / Creativity (Blog writing / Vlogging, etc.)
3. Pre/Post - Experiment Test / Viva / Experimental Write-Up for each Experiment, Day to Day Experiments / Assignments / Tutorials / Power point presentations / Design thinking / Quiz / Seminar / Case studies / Design Thinking / Innovation / Creativity (Blog writing / Vlogging, etc.) [Lab Component]
4. End Semester Examinations [Theory and Lab components]
INDIRECT Assessment
1. Course end survey
2. Activity based survey [if any]

Detailed Syllabus

Module	Hours	Course Outcome
Module 1: Introduction to Ethical Hacking	15	CO1
1.1 Information Security Overview: Cyber Kill Chain Concepts, Hacking Concepts, Ethical Hacking Concepts, Information Security Controls, Information Security Laws and Standards. 1.2 Footprinting and Reconnaissance: Footprinting Concepts, Footprinting Countermeasures 1.3 Scanning Networks: Network Scanning Concepts, Scanning Tools 1.4 Enumeration: Enumeration Concepts, NetBIOS Enumeration, SNMP Enumeration, LDAP Enumeration, Enumeration Countermeasures 1.5 Vulnerability Analysis: Vulnerability Assessment Concepts, Vulnerability Assessment Tools, Vulnerability Assessment Reports		
Module 2: Cybersecurity Attacks and Defense Mechanisms	15	CO2
2.1 System Hacking: System Hacking Concepts, Cracking Passwords, Escalating Privileges, Maintaining Access, Clearing Logs, Password Cracking, Password Attacks, steganography, Steganography Tools, Steganalysis, Steganography Detection Tools 2.2 Malware Threats: Malware Concepts, Advanced Persistent Malware, Trojan Concepts, Virus and Worm Concepts, Countermeasures 2.3 Sniffing: Sniffing Concepts, Spoofing Attacks, Sniffing Tools, Countermeasures 2.4 Social Engineering: Social Engineering Concepts, Social Engineering Techniques, Countermeasures 2.5 SQL Injection: SQL Injection concepts, SQL Injection Countermeasures.		
Module 3: Network Intrusions and Web Exploitation Techniques	15	CO3
3.1 Denial-of-Service: DoS/DDoS Concepts, DoS/DDoS Attack Tools, Countermeasures 3.2 Session Hijacking: Session Hijacking Concepts, Session Hijacking Tools, Countermeasures 3.3 Evading IDS, Firewalls, and Honeypots: IDS, IPS, and Firewall Concepts, IDS/Firewall Evasion Countermeasures 3.4 Hacking Web Applications: Hacking Web Applications, Threats, Hacking Methodology, Web Application Security		
Module 4: Emerging Technologies and Cybersecurity Regulations	15	CO4
4.1 Hacking Wireless Networks: Wireless Concepts, Wireless Encryption, Threats, Hacking Methodology, Attack Countermeasures. 4.2 IoT Hacking: IoT Concepts and Attack, IoT Hacking Methodology, Attack Countermeasures 4.3 Cloud Computing: Cloud Computing Concepts, Cloud Computing Threats , Cloud Security 4.4 Cryptography: Cryptography Concepts and Encryption Algorithms, applications of Cryptography, Cryptanalysis Methods and Cryptography Attacks , Cryptography Attack Countermeasures.		
Self Learning: IIT Hacking, Microsoft Azure Hacking, Google Cloud Hacking		

Exercises: 0 Hrs/Week	Total Hours: 60

Lab Component:

Suggested list of experiments (From the given list of topics, participants may fix case study/scenario based experiments like the one shown in Experiment 1):

S.No.	Experiment Title	Course Outcomes
1	To investigate digital footprints and metadata of a suspicious file and correlated online activity to determine the identity of a potential insider threat. E.g. for case study/scenario: A confidential company document was leaked online. The cybersecurity team suspects an insider has exfiltrated the file. The team discovered: • The leaked document (e.g. docx file) from a file-sharing site. • A suspicious IP address found in internal logs linked to social media activity. • Several social media posts made shortly after the file was leaked. As the forensic investigator team analyze both the metadata of the file and online presence of the user to build a digital footprint.	CO1
2	Practical Investigative procedures including logging and tagging evidence, following chain of custody and photographing evidences on the scene.	CO2
3	Perform Vulnerability Assessment using Various Vulnerability Assessment Tools (Software/ Network)	CO3
4	Perform an Active Online Attack to Crack the System's Password.	CO3
5	Use Steganography to Hide Data. Recommended Tools: Steghide (Linux/Mac), OpenStego, Stegosuite.	CO2
6	Explore Social Engineering attacks using SET Toolkit.	CO2
7	Detect SQL Injection Vulnerabilities using Various SQL Injection Detection Tools.	CO3
8	Perform DoS and DDoS attack on target system.	CO3
9	Perform Session Hijacking using various tools.	CO3
10	IDS Evasion using Nmap Decoy Scan.	CO3
11	Exploiting OWASP Top 10 Vulnerabilities in DVWA.	CO4
12	Detect and Exploitation of IoT Devices Using Shodan.	CO4
13	Perform File and Text Message Encryption.	CO4
14	Perform Cryptanalysis using Various Cryptanalysis Tools.	CO5

Practical: 4 Hrs/Week	Total Hours: 120

Text Books

Sr. No	Title	Edition	Authors	Publisher	Year
1	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
2	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
3	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
4	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
5	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Reference Books

Sr. No	Title	Edition	Authors	Publisher	Year
1	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
2	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Online References

Sr. No	Website Name
1	[illegible]

Program:	Second Year B.Des (Semester IV)	L	P	C
Internship/Industry Visit:	Course Code: BVUXXIIIID0444		0	2

Course Objective No.	Objective Description
1	To integrate academic knowledge with practical industry experience through real-time projects.
2	To observe professional practices, workflows, and organizational structures in a real-world setting.
3	To participate in problem-solving activities and collaborative team efforts within the organization.
4	To document professional learning, challenges faced, and technical contributions during the internship period.

CO / No.	Course Outcome Description
CO1	Apply theoretical concepts to practical scenarios encountered during industrial exposure.
CO2	Contribute to the design, development, or testing phases of live projects under professional supervision.
CO3	Communicate technical findings, progress, and project outcomes effectively in written and verbal form.
CO4	Reflect on professional growth, ethical considerations, and skill development achieved through training.

DIRECT Assessment
1. Continuous Internal Assessment (Theory component)
2. Assignments/Tutorials/Power point presentation/Group discussion/Quiz/seminar/Case studies/ Design Thinking/Innovation/Creativity/Blog writing/Blogging, etc)
3. Oral/Viva - Experiments/Viva/Viva, Experimental Skills (To be made Appropriate, One on One Experiments/Assignments/Tutorials/Power point presentation/Group discussion/Quiz/seminar/ Case studies/Design Thinking/Innovation/Creativity/ Blog writing/Blogging, etc) (Lab Component)
4. End Semester Examination (Theory and Lab component)
INDIRECT Assessment
1. Course-end survey
2. Alumni/Industry survey (If any)

Programs	Second Year B.Voc (Semester IV)	L	T	C
UI/UX Design (Choose Any One) 1. Google Cloud Computing Foundations with Kubernetes (NEW) 2. Cloud Administration Analyst (SSC/Q0904) 3. Data Scientist (SSC/Q0101) 4. Product Manager – Web & Mobile (SSC/Q0901) 5. Application Architect – Web & Mobile (SSC/Q0902) 6. Any Other with NSQF Level-6	Course Codes: BVCT0B0B0B0P(10)	-	-	05

Sr. No.	UI/UX Design (Choose Any One)	Syllabus for this qualification Pack is available on: -
1	Google Cloud Computing Foundations with Kubernetes (NEW)	SSC/Q0903 (NEW) – Qualification Pack
2	Cloud Administration Analyst (SSC/Q0904)	SSC/Q0904 (NEW) – Qualification Pack
3	Data Scientist (SSC/Q0101)	SSC/Q0101 (NEW) – Qualification Pack
4	Product Manager – Web & Mobile (SSC/Q0901)	SSC/Q0901 (NEW) – Qualification Pack
5	Application Architect – Web & Mobile (SSC/Q0902)	SSC/Q0902 (NEW) – Qualification Pack
6	Any Other with NSQF Level-6	