Shri Vile Parle Kelavani Mandal's

Dwarkadas J. Sanghvi College of Engineering

(Autonomous College Affiliated to the University of Mumbai)

Scheme and detailed syllabus

Final Year B.Tech

in

DJS22 Honors Program in Smart Computing

(Semester VIII)

Prepared by:- Board of Studies in Computer Science and Engineering (IoT and Cyber Security with Block Chain Technology)

With effect from the Academic Year: 2025-2026

Department of Computer Science and Engineering (IoT and Cyber Security with Block Chain Technology)

Proposed Scheme for Honors Degree Program in Smart Computing   SEMESTER:VIII   (Autonomous)

(Academic Year 2025-2026)

Sr. No.	Course Code	Course	Teaching Scheme				Semester End Examination (SEE) -					Continuous Assessment (A)					Aggregate (A+B)	Credits	
			Theory (Hrs)	Practical (Hrs.)	Tutorial (Hrs.)	Credits	Duration (Hrs)	Theory	Oral	Pract	Oral & Pract	SEE Total (A)	Term Test 1 (TT1)	Term Test 2 (TT2)	Total (TT1 + TT2)	Term work	CA Total (B)			
	SEM V																			
1	DJS22ICHN1C1	Smart Technologies	4	--	--	4	2	65	--	--	--	65	20	15	35	--	35	100	4	4
	SEM VI																			
2	DJS22ICHN1C2	Cognitive Computing	4	--	--	4	2	65	--	--	--	65	20	15	35	--	35	100	4	5
	DJS22ICHN1L1	Cognitive Computing Laboratory	--	2	--	1	2	--	25	--	--	25	--	--	--	25	25	50	1	
	SEM VII																			
3	DJS22ICHN1C3	Human Computer Interaction	4	--	--	4	2	65	--	--	--	65	20	15	35	--	35	100	4	5
	DJS22ICHN1L2	Human Computer Interaction Laboratory	--	2	--	1	2	--	25	--	--	25	--	--	--	25	25	50	1	
	SEM VIII																			
4	DJS22ICHN1C4	Social Cybersecurity	4	--	--	4	2	65	--	--	--	65	20	15	35	--	35	100	4	4
		Total	16	4	0	18	12	260	50	0	0	310	80	60	140	50	190	500	18	

Prepared by   **Checked by**   **Head of the Department**   **Vice Principal**   **Principal**

Program: B.Tech in Computer Science and Engineering (IoT and Cybersecurity with Block chain Technology)	Final Year B.Tech	Semester: VIII
Course : Social Cybersecurity	Course Code: DJS22ICHN1C4	

Teaching Scheme (Hours / week)				Evaluation Scheme							
				Continuous Assessment Marks (A)			Semester End Examination Marks (B)				Total marks (A+B)
Lectures	Practical	Tutorial	Total Credits	Term Test 1	Term Test 2	Total	Theory				
				20	15	35	65				100
				Laboratory Examination			Term work				
4	--	--	4	Laboratory Work	Tutorial / Mini project / presentation/ Journal/ Practical	Total Term work	Oral	Practical		Oral & Practical	--
				--	--	--	--	--		--	

Prerequisite:
1. Computer Networks
2. Applied Cryptography

Course Objectives: The objective of the course is
1. Provide students with a comprehensive understanding social networks and related security challenges.
2. Equip students with the ability to identify cyber threats and attacks on social media.
3. Familiarize students with the role of social media in digital forensics
4. Enable students to design effective security mechanisms to safeguard user data and mitigate risks in social networks.

Course Outcomes: On completion of this course, learners will be able to:

1. Identify key security risks, privacy issues, and vulnerabilities in social networking platforms.
2. Explain emerging challenges and evolving threat landscapes impacting social networks.
3. Analyze various cyber threats, attack techniques, and incident patterns affecting social media.
4. Evaluate digital forensic techniques used for examining and interpreting social media data.
5. Describe authentication mechanisms, data protection measures, and privacy frameworks relevant to social network security.
6. Assess the role of user awareness, policies, and best practices in strengthening social network security.

Detailed Syllabus:

Unit	Description	Duration
1	**Introduction to Social Networking Security** **Overview of Social Networks**: Definition and Types of Social Networks, The Evolution of Social Media Platforms Web 1.0 to Web 3.0, User Behavior and Interactions in Social networks **Security and Privacy Threats**: Cyberbullying, Cyberstalking, Honey Trapping, Trolling, Account Hijacking and Impersonation, Fake Engagement, Data Scraping, Doxxing and, Third-Party Integrations. **Importance of Social Network Security**: Impact of Security Breaches on Users and Organizations, Case Studies of Notable Security Incidents in social media	08
2	**Cyber Threats and Attacks in Social Networks** **Cyber Threats and Attacks:** Social Engineering Attacks: Techniques and Prevention, Malware Distribution through Social Media Platforms, Location Tracking and Privacy, Fake Accounts and Bots: Identification and Implications **Social Media Manipulation and Misinformation:** Spread of Fake News and Its Consequences, Case Studies: Analyzing Social Media Campaigns and their Effects **Responding to Cyber Threats:** Incident Response Strategies for Social Network Security, Crisis Management in the Wake of a Security Breach	08
3	**Privacy and Data Protection in Social Networks** **User Privacy on Social Networks:** The role of data collection, tracking, and targeted advertising, user consent; privacy policies; and the risks of oversharing. **Data Protection Mechanisms:** Techniques for Protecting User Data: Encryption and Anonymization, Compliance with Data Protection Regulations. Privacy Settings and Controls on Major Platforms, Data Minimization and User Consent **Privacy Risks and Vulnerabilities**: Identifying and Mitigating Risks Associated with User Data, The Role of Third-Party Apps in Data Leakage	07
4	**Social Media and Digital Forensics** **Role of social media in Digital Forensics**: The Importance of Social Media Data in Investigations, Types of Evidence Available on social media. **Data Extraction Techniques:** Manual and Automated Data Collection Methods APIs and Web Scraping for Data Extraction **Processing and Analyzing Social Media Data**: Data Cleaning and Transformation Techniques - Tools for Data Analysis: Sentiment Analysis and Text Mining	07

5	**Security Mechanisms for Social Networks** **User Authentication Methods:** OAuth 2.0 and Single Sign-On (SSO) **Threat Detection and Prevention:** AI and Machine Learning for Threat Detection - Real-Time Monitoring and Incident Response Solutions **Content Moderation and Policy Enforcement:** Techniques for Identifying Harmful Content - Community Guidelines and Enforcement Mechanisms	06
6	**Future Trends and Challenges in Social Networking Security** **Emerging Technologies and Challenges:** Evolving Threat Landscape: Digital Arrest, Deepfakes and Disinformation Privacy Concerns with New Features and Technologies, Case Studies on Digital Arrest, Deepfakes. **Best Practices for Social Network Security:** Regulatory Frameworks: Overview of GDPR (General Data Protection Regulation), CCPA (California Consumer Privacy Act) and their implications on social networks, Developing a Security Culture among Users	06
	Total	42

Books Recommended:

Text Books:

1. Brij B. Gupta, Somya Ranjan Sahoo "Online Social Networks Security Principles, Algorithm, Applications, and Perspectives" CRC Press, ISBN:9781000347197 (2021)
2. Tanmoy Chakraborty, "Social Network Analysis", First Edition, Wiley, 2021.
3. Michael Cross "Social Media Security" Syngress ISBN: 9781597499873 (2013)

Web resources:

1. Online Training on social media and Cybersecurity [available online] https://ciet.ncert.gov.in/activity/smcs
2. online training on Social Media Safety and Well-being [available online] https://ciet.ncert.gov.in/activity/swbe

Online Courses: NPTEL / Swayam:

1. Privacy and Security in Online Social Media by Prof. Ponnurangam Kumaraguru IIIT Hyderabad https://onlinecourses.nptel.ac.in/noc23_cs13/preview

2. Social Network Analysis by Prof. Tanmoy Chakraborty IIT Delhi https://onlinecourses.nptel.ac.in/noc24_cs90/preview

Evaluation Scheme:

Continuous Assessment (A):

Theory:

1. One term test of 20 marks and one term test/presentation/assignment/course project/Group discussion/

   any other of 15 marks will be conducted during the semester.

2. Total duration allotted for writing Term Test 1 paper is 1 hr.

3. Total duration allotted for writing Term Test 2 paper is 45 minutes.

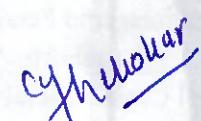**Semester End Examination (B):**

Theory:

1. Question paper will be based on the entire syllabus summing up to 65 marks.

2. Total duration allotted for writing the paper is 2 hrs.

| Prepared by | Checked by | Head of the Department | Vice Principal | Principal |