



Shri Vile Parle Kelavani Mandal's
DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING
(Autonomous College Affiliated to the University of Mumbai)
NAAC Accredited with "A" Grade (CGPA : 3.18)



Shri Vile Parle Kelavani Mandal's
Dwarkadas J. Sanghvi College of Engineering
(Autonomous College Affiliated to the University of Mumbai)

Scheme and Detailed Syllabus
of
DJ19 Honors Program
in
Smart Computing

With effect from the Academic Year: 2024-2025



Scheme for Honors in Smart Computing (Academic Year 2024-2025)

Sr	Course Code	Course	Teaching Scheme(hrs.)				Continuous Assessment (A)			Semester End Assessment (B)					Aggregatee (A+B)	Total Credits
			Th	P	T	Credits	Th	T/W	Total CA (A)	Th	O	P	O &P	Total SEA (B)		
SEM V																
1	DJ19ICCHN1C1	Smart Technologies	4	--	--	4	25	--	25	75	--	--	--	75	100	4
SEM VI																
2	DJ19ICCHN1C2	Cognitive Computing	4	--	--	4	25	--	25	75	--	--	--	75	100	4
3	DJ19ICCHN1L2	Cognitive Computing Laboratory	--	2	--	1	--	25	25	--	--	--	25	25	50	1
SEM VII																
4	DJ19ICCHN1C3	IoT Data Analytics	4	--	--	4	25	--	25	75	--	--	--	75	100	4
5	DJ19ICCHN1L3	IoT Data Analytics Laboratory	--	2	--	1	--	25	25	--	--	--	25	25	50	1
SEM VIII																
7	DJ19ICCHN1C4	Social Cybersecurity	4	--	--	4	25	--	25	75	--	--	--	75	100	4
		Total	16	4	0	18	100	50	150	300	0	0	50	350	500	18

Cy Jhuken



Program: B.Tech. in Computer Science and Engineering (IoT and Cyber Security with Block Chain Technology)				Final Year		Semester: VIII			
Course : Social Cybersecurity				Course Code: DJ19ICCHN1C4					
Teaching Scheme (Hours / week)				Evaluation Scheme					
				Semester End Examination Marks (A)			Continuous Assessment Marks (B)		
Lectures	Practical	Tutorial	Total Credits	Theory			Term Test 1	Term Test 2	Average
				75	25	25	25	100	
				Laboratory Examination			Term work		Total Term work
				Oral	Practical	Oral & Practical	Laboratory Work	Tutorial / Mini project / presentation / Journal	
4	--	--	4	--	--	--	--	--	--

Pre-requisite:

1. Computer Networks
2. Applied Cryptography
3. Security in computing
4. Mobile Device Security and Forensics

Objectives:

1. Provide students with a comprehensive understanding of security and privacy challenges on social media platforms.
2. Equip students with the ability to identify and analyze various cyber threats and attacks targeting social networks.
3. Familiarize students with the role of social media in digital forensics, including data extraction and analysis techniques.
4. Enable students to design and implement effective security mechanisms to safeguard user data and mitigate risks in social networks.

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

1. Identify and assess security risks and privacy challenges in social networking environments.
2. Demonstrate the ability to evaluate and respond to cyber threats and incidents affecting social media platforms.
3. Acquire skills in extracting and analyzing social media data for digital forensic investigations.
4. Capable of implementing user authentication and data protection measures in social networking contexts.
5. Discuss emerging trends and challenges in social networking security, including the implications of new technologies.
6. Discuss best practices and policies to enhance security awareness among users of social media platforms.

Handwritten signatures and initials in blue ink.



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	07
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

9/15



Shri Vile Parle Kelavani Mandal's

DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING

(Autonomous College Affiliated to the University of Mumbai)

NAAC Accredited with "A" Grade (CGPA : 3.18)



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: Deepfakes and Disinformation - Privacy Concerns with New Features and Technologies 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	04
Total		39

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 IIT 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:

Semester End Examination (A):

Theory:

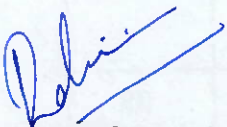
1. Question paper will be based on the entire syllabus summing up to 75 marks.
2. Total duration allotted for writing the paper is 3 hrs.

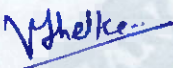


Continuous Assessment (B):

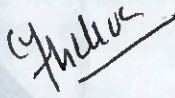
Theory:

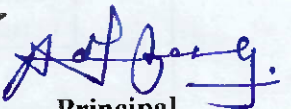
1. Two term tests of 25 marks each will be conducted during the semester out of which; one will be a compulsory term test (on minimum 03 Modules) and the other can either be a term test or an assignment on live problems or a course project.
2. Total duration allotted for writing each of the paper is 1 hr.
3. Average of the marks scored in both the two tests will be considered for final grading


Prepared by


Checked by


Head of the Department


Vice Principal


Principal

