Agnel Charities'

Fr. C. Rodrigues Institute of Technology

Sector 9A, Vashi, Navi Mumbai, 400703, Maharashtra, India

www.fcrit.ac.in

An Autonomous Institute Affiliated to the University of Mumbai

Curriculum & Examination Schemes
for

Honours / Minor / Honours in Research
Degree Programs in Cyber security & Data Science offered by Information Technology

Approved By: Academic Council of Fr. C. Rodrigues Institute of Technology

Revision: N2024.1

Effective from :2025-26

A. Abbreviations

HMC	Honours or Minor Core Course
HML	Honours or Minor Laboratory
HMP	Honours or Minor Mini Project
RPR	Research Project
RPC	Research Project Coursework

Proposed Honours / Minor Degree specializations offered by Department of Information Technology are as follows.

a) Cyber Security
b) Data Science

Mapping as 'Honours' or 'Minor' Degree Program with Existing B. Tech Programs offered by Department of Information Technology

Sr. No.	Honours/Minor Specialization	B. Tech Programs that can offer this as an Honours Degree	B. Tech Programs that can offer this as a Minor Degree
a)	Cyber Security	1. Computer Engineering 2. Electronics & Telecommunication Engineering 3. Information Technology	1. Mechanical Engineering 2.Electrical Engineering
b)	Data Science		

a) Cyber Security

Curriculum Structure for Honours/Minor Degree Program in Cyber Security

Course Type	Sem	Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
				L	P	T	L	P	T	Total
HMC	V	HMCCS501	Cybercrime & Cyber Security	3	--	--	3	--	--	3
HMC	VI	HMCCS602	Infrastructure Security	3	--	--	3	--	--	3
HMC	VII	HMCCS703	Security Audit & Risk Assessment	4	--	--	4	--	--	4
HML	VII	HMLCS701	Cyber Security Laboratory	--	4	--	--	2	--	2
HMC	VIII	HMCCS804	Application Security	4	--	--	4	--	--	4
HMP	VIII	HMPCS801	Honours/Minor Mini Project	--	6	--	--	2	--	2
			Total	**14**	**10**	**--**	**14**	**04**	**--**	**18**

Examination Scheme for Honours/Minor Degree Program in Cyber Security

Examination Scheme									
Course Type	Sem	Course Code	Course Name	In-Semester Assessment		End Sem Exam (ESE)	Exam. Duration for Theory (in Hrs)		Total
				Continuous Assessment	Mid Sem Exam		Mid Sem	End Sem	
HMC	V	HMCCS501	Cybercrime & Cyber Security	20	30	50	1.5	2	100
HMC	VI	HMCCS602	Infrastructure Security	20	30	50	1.5	2	100
HMC	VII	HMCCS703	Security Audit & Risk Assessment	20	30	50	1.5	2	100
HML	VII	HMLCS701	Cyber Security Laboratory	50	--	--	--	--	50
HMC	VIII	HMCCS804	Application Security	20	30	50	1.5	2	100
HMP	VIII	HMPCS801	Honours/Minor Mini Project	50	--	50	--	--	100
			Total	**180**	**120**	**250**	**--**	**--**	**550**

b) Data Science

Curriculum Structure for Honours/Minor Degree Program in Data Science

Course Type	Sem	Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
				L	P	T	L	P	T	Total
HMC	V	HMCDS501	Foundation of Data Science	3	--	--	3	--	--	3
HMC	VI	HMCDS602	Data Science for Healthcare	3	--	--	3	--	--	3
HMC	VII	HMCDS703	Social Media Analytics	4	--	--	4	--	--	4
HML	VII	HMLDS701	Data Analytics Laboratory	--	4	--	--	2	--	2
HMC	VIII	HMCDS804	Marketing & Financial Analytics	4	--	--	4	--	--	4
HMP	VIII	HMPDS801	Honours/Minor Mini Project	--	6	--	--	2	--	2
			Total	**14**	**10**	**--**	**14**	**04**	**--**	**18**

Examination Scheme for Honours/Minor Degree Program in Data Science

Examination Scheme									
Course Type	Sem	Course Code	Course Name	In-Semester Assessment		End Sem Exam (ESE)	Exam. Duration for Theory (in Hrs)		Total
				Continuous Assessment	Mid Sem Exam		Mid Sem	End Sem	
HMC	V	HMCDS501	Foundation of Data Science	20	30	50	1.5	2	100
HMC	VI	HMCDS602	Data Science for Healthcare	20	30	50	1.5	2	100
HMC	VII	HMCDS703	Social Media Analytics	20	30	50	1.5	2	100
HML	VII	HMLDS701	Data Analytics Laboratory	50	--	--	--	--	50
HMC	VIII	HMCDS804	Marketing & Financial Analytics	20	30	50	1.5	2	100
HMP	VIII	HMPDS801	Honours/Minor Mini Project	50	--	50	--	--	100
			Total	**180**	**120**	**250**	**--**	**--**	**550**

Course Type	Course Code	Course Name	Credits
HMC	HMCCS501	CYBERCRIME AND CYBERSECURITY	03

Examination Scheme					
Distribution of Marks			Exam Duration (Hrs.)		Total Marks
Continuous Internal Evaluation		End Semester Exam			
Internal Evaluation	Mid-Sem Exam		MSE	ESE	
20	30	50	1.5	2	**100**

Pre-requisite :

NIL

Program Outcomes addressed :

1. PO1: Engineering knowledge
2. PO2: Problem analysis
3. PO3: Design/development of solutions
4. PO5: Engineering tool usage
5. PO6:The Engineer and The World
6. PO7:Ethics
7. PO11:Life-Long Learning

Course Objectives :

1. To create awareness to the learner regarding the threat landscape leading to need of understanding the fundamentals of cybersecurity and preventive measures
2. To make the learners correlate the different types of cybercrime to the attack strategy by the cybercriminals.
3. To make the learners better acquainted with the legal aspects pertaining to cybercrime and the corresponding IT Act reforms and amendments.
4. To familiarize the learners with steps of ethical hacking, cryptography, the methodologies and techniques of Sniffing techniques, tools, and ethical issues.
5. To acquaint the learners with the significance of digital forensic lifecycle in effect identifying the data in case of any incident handling.
6. To upskill the learner in identifying the network, mobile ,newer technologies threats and identifying the appropriate tools to mitigate them.

Module	Details	Hrs
00.	**Course Introduction** Cybercrime and cybersecurity are the foundation course to delve into the domain of security in the cyberspace with respect to the different technologies under the attacks by the malicious intruders, the response strategy to the attack and steps to mitigate, investigate the cybercrime	**01**
01.	**Fundamentals of Cybersecurity:** ***Learning Objective:*** *To evaluate the relevance of cybersecurity along with the challenges in the growing threat landscape, essence of securing the information and be aware of the evolution of cybersecurity.*	**05-07**
	Contents: **Importance of Cybersecurity:** History of Data Breaches, Understanding the attack surface, Threat Landscape, Importance of securing Network and Application, **Information Assurance Fundamentals:** Authentication, Authorization, Nonrepudiation, Confidentiality, Integrity, Availability, Layers of Cybersecurity, **Evolution of Cybersecurity:** Cyberwarfare, cybercrime, Cyberterrorism, Challenges of Cybersecurity	
	Self-Learning Topics: *Identify the different use cases of threats to the non-adherence of information assurance* ***Learning Outcomes :*** *A learner will be able to* *LO 1.1: Apply computer science theory to interpret threats and their mitigation steps, and use engineering fundamentals to understand the necessity of securing networks and applications in real-world scenarios. (P.I-1.4.1, P.I-1.3.1)* *LO 1.3: Produce the concept of information assurance to design and implement the secure systems (P.I-3.2.2)* *LO 1.4: Define the problem and its solution in ensuring security in each layer of the cyber sphere (P.I-3.1.1)* *LO 1.5: Arrive at the conclusions to Infer the layers of cybersecurity to summarize the conclusions of requirement of each layer of security (P.I-2.4.4)* *LO 1.6:Identify the challenges for providing security to the application , network (P.I-2.4.3)*	
02.	**Cybercrime and Cyber Offenses** ***Learning Objectives:*** *To be able to classify the cybercrime, outline the steps involved in planning a cybercrime and explain social engineering. Botnets ,attack vector.*	**07-09**
	Contents: Classification of Cybercrimes, Hacker, Cracker, Phreaker, Cyber offenses: Categories of Cybercrime, Criminals strategy for planning attacks, Social Engineering, Cyberstalking, Botnets, Attack Vector, Cybercrime and Cloud Computing	

	Self-Learning Topics: *Different tools in analyzing cybercrime* ***Learning Outcomes :***	
	A learner will be able to *LO 2.1: Apply the theory and principles of computer science engineering to classify cybercrime methods, identify ethical and unethical hacker conduct, and compare and contrast hackers, crackers, and phreakers. (P.I-1.4.1, P.I-6.3.1)* *LO 2.2: Evaluate the planning stages of a cybercrime to identify potential vulnerabilities, and analyze the steps involved in planning a cybercrime. Describe how engineering roles can develop preventive measures to protect the public interest at global, regional, and local levels. (P.I-6.1.1, P.I-2.1.1)* *LO 2.3: Interpret legislation and codes of conduct in cybercrime scenarios, examine social engineering attack outcomes, and apply ethical principles to propose responses. Use engineering fundamentals to explain cyberstalking, attack vectors, cybercrime, and cloud computing. (P.I-6.2.1, P.I-6.4.2, P.I-1.3.1)*	
03.	**Cybercrime and Cybersecurity: The Legal Outlook** ***Learning Objective:*** *To comprehend the importance of the cyber law with pertaining increase of threats in cyberspace, familiarize with the Indian IT Act and its amendments*	**07-09**
	Contents: **The Indian IT Act**: Admissibility of Electronic Records, Positive aspects of the ITA 2000, Weak Areas of the ITA 2000, **Amendments to the Indian IT Act:** Overview of Changes made to Indian IT Act, State Government Powers Impacted by the Amendments, Impact of IT Act Amendments of IT Organization, Cybercrime and Punishments	
	Self-Learning Topics: *Cybercrime and Federal laws in different countries..* ***Learning Outcomes :*** *A learner will be able to* *The learner will be able to* *LO 3.1: Evaluate problem statements to identify objectives while analyzing and describing the Indian IT Act, 2000, in relation to various cybercrimes and the corresponding cyber laws that address them ((P.I 2.1.1,6.1.1, 6.2.1).* *LO 3.2: Analyze crime scenarios to identify objectives and arrive at conclusions while corelating the amendments in the IT Act, 2008, in comparison to the IT Act, 2000 (P.I-2.4.4,6.2.1)* *LO 3.3: Analyze the shortcomings in implementing the IT Act for appropriate punishment and its impact on IT organizations while identifying solution limitations, sources, and causes to the crime. (P.I-2.4.3,7.1.1,7.2.2),*	
04.	**Ethical Hacking** ***Learning Objective:*** *To acquaint themselves to the steps of ethical hacking , cryptographic techniques and the various tools utilized to simulate and identify the cyberattack.*	**08-10**
	Contents:	

	Steps of ethical hacking, Demonstration of Routing Protocols using Cisco Packet Tracer, Cryptographic Hash Functions & applications, steganography, biometric authentication, lightweight cryptographic algorithms. Demonstration of various cryptographic tools and hashing algorithms, Study of various tools for Network Security such as Wireshark, John the Ripper, Metasploit, etc.	
	Self-Learning Topics: *Ransomware(Wannacry), Rootkits, Mobile device security*	
	Learning Outcomes: *The learner will be able to* *LO 4.1: Apply engineering fundamentals to outline the steps of ethical hacking and use Cisco Packet Tracer to implement routing protocols, analyze, and draw conclusions from the traced packet ((P.I-1.3.1,2.4.4,4.3.1).* *LO 4.2: Apply computer science engineering principles to illustrate cryptographic techniques and steganography while selecting suitable steganographic methods, biometric authentication, and lightweight cryptographic algorithms based on the problem (P.I-1.4.1,4.1.2).* *LO 4.3: Identify cryptographic tools and hashing algorithms while demonstrating proficiency in analyzing various network security tools and their applications (P.I-5.1.1,5.2.2).*	
05.	**Digital Forensics** ***Learning Objective/s:*** *To know the techniques of identifying digital evidence, the investigation techniques of cybercrime, investigation on network and mobile using the appropriate tools ..*	**07-09**
	Contents: Cyber forensics and Digital Evidence, Digital Forensics Lifecycle, Chain of Custody, Incident Response Process, **Network Forensics:** Sources of Network-Based Evidence, Evidence Acquisition, Analyzing Network Traffic: Packet Flow and Statistical Flow, **Mobile Forensics**: Mobile phone evidence extraction, Procedure for Handling an Android Device, Imaging Android USB Mass Storage Devices. .	
	Self-Learning Topics: *Elcomsoft iOS Forensic Toolkit, Remo Recover tool for Android Data recovery*	
	Learning Outcomes : *A learner will be able to* *LO 5.1: Analyze digital evidence based on the scene to identify and arrive at conclusions while evaluating and interpreting the incident response process by identifying objectives for the strategy (P.I-2.4.4,2.1.1)* *LO 5.2: Use the appropriate strategy for the investigation procedure up to the trial of the case (P.I-4.3.1)* *LO 5.3: Apply engineering fundamentals to infer the analysis methodology for network traffic and define and analyze different sources of network evidence to understand their relevance to the cybercrime (P.I-1.3.1,4.1.1)* *LO 5.4: Apply theory of computer science engineering to Outline the procedure for extracting evidence from the mobile (P.I-1.4.1)*	

06.	**Cybersecurity Technologies** ***Learning Objectives:*** *To understand the relevant security implementation with implementation of the newer technologies.*	**03-05**
	Contents:	
	Advanced data security, Modern day regulations, Incidence response and forensics, Enterprise security at scale, Penetration testing, DevSecOps, IoT security, User behavior analytics, Endpoint detection and response (EDR)	
	Self-Learning Topics: *Different techniques utilized to provide security in recent technologies* ***Learning Outcomes:*** *A learner will be able to* *LO 6.1: Define the purpose of mobile security, cloud security, enterprise security to ensure threat mitigation (P.I-4.1.1)* *LO 6.2: Arrive at conclusions by inferring the existing methods utilized to provide security to recent technologies (P.I-2.4.4)* *LO 6.3: Identify and choose the appropriate security techniques to be utilized in DevOps, IOT domains according to the problem statement (P.I-4.1.2)* *LO 6.4:Evaluate the concept of user behavior analytics to detect the threat user (P.I-2.1.1)*	
	Course Conclusion	**01**
	Total	**45**

Performance Indicators:

P.I. No.	P.I. Statement
1.3.1	Apply engineering fundamentals.
1.4.1	Apply theory and principles of computer science engineering to solve an engineering problem.
2.1.1	Evaluate problem statements and identifies objectives
2.4.3	Identify the limitations of the solution and sources/causes.
2.4.4	Arrive at conclusions with respect to the objectives.
3.2.2	Ability to produce a variety of potential design solutions suited to meet functional requirements.
4.1.1	Define a problem for purposes of investigation, its scope and importance
4.1.2	Ability to choose appropriate procedure/algorithm, data set and test cases.
4.3.1	Use appropriate procedures, tools and techniques to collect and analyze data
5.1.1	Identify modern engineering tools, techniques and resources for engineering activities
5..2.2	Demonstrate proficiency in using discipline specific tools

6.1.1 Identify and describe various engineering roles; particularly as pertains to protection of the public and public interest at global, regional and local level

6.2.1 Interpret legislation, regulations, codes, and standards relevant to your discipline and explain its contribution to the protection of the public

6.3.1 Identify risks/impacts in the life-cycle of an engineering product or activity

6.4.2 Apply principles of preventive engineering and sustainable development to an engineering activity or product relevant to the discipline

7.1.1 Identify situations of unethical professional conduct and propose ethical alternatives

7.2.2 Examine and apply moral & ethical principles to known case studies

Course Outcomes:

Learner will be able to

1. Analyse the threat landscape across different layers of cybersecurity and evaluate its impact on information assurance frameworks. (LO *1.1, LO 1.2, LO 1.3, LO 1.4, LO 1.5, LO 1.6)*
2. Examine various cybercrimes, assess their attack strategies, and analyse their alignment with existing cyber laws and regulations.(*LO 2.1,LO 2.2,LO 2.3, LO 3.1,3.2,LO 3.3*)
3. Evaluate ethical hacking principles in real-world scenarios and critically analyze the effectiveness of tools used for threat mitigation.(*LO 4.1,LO 4.2,LO 4.3)*
4. Analyse a cybercrime scene, identify key digital evidence, and perform detailed forensic analysis to derive meaningful insights.(*LO 5.1,LO 5.2,LO 5.3,LO 5.4)*
5. Assess emerging cybersecurity requirements in evolving technologies and analyze their integration into secure development frameworks. (*LO 6.1, LO 6.2, LO 6.3, LO 6.4*)

CO-PO Mapping Table with Correlation Level

CO ID	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
HMCCS501.1	3	3	3	-	-	-	-	-	-	-	-
HMCCS501.2	3	-	-	-	-	3	3	-	-	-	-
HMCCS501.3	3	-	-	3	3	-		-	-	-	-
HMCCS501.4	3	3	-	3	-	-	-	-	-	-	-
HMCCS501.5	-	3	-	3	-	-	-	-	-	-	-
Average	**3**	**3**	**3**	**3**	**3**	**3**	-	**3**		-	-

-

Text Books :

1. Computer Security Principles and Practice ,William Stallings, Seventh Edition, 2017, Pearson Education

2. Nina Godbole and SunitBelpure, Cyber Security Understanding Cyber Crimes,Computer Forensics and Legal Perspectives,First Edition,2011,Wiley
3. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, 2011, CRCPress.
4. Security in Computing -- Charles P. Pfleeger, Fifth Edition,2015, Pearson Education
5. Android Forensics : Investigation, Analysis, and Mobile Security for Google Android by Andrew Hogg, 2011, Elsevier Publication

Reference Books :

1. Incident Response & Computer Forensics by Jason T. Luttgens, Matthew Pepe and Kevin Mandia, Third Edition,2014,McGraw-Hill Education,
2. Network Forensics : Tracking Hackers through Cyberspace by Sherri Davidoff and Jonathan Ham, 2012,Pearson Education
3. Practical Mobile Forensic by Satish Bommisetty, Rohit Tamma, Heather Mahalik, PACKT publication, Open source publication, 2014 ISBN 978-1-78328-831-1
4. Advanced Computer Architecture: Parallelism, Scalability, Programmability, Kai Hwang, Naresh Jotwani, Third Edition, 2017, McGraw Hill Education.

Other Resources :

1. Ethical Hacking ,By Prof. Indranil Sengupta , Department of Computer Science and Engineering IIT Kharagpur, Web Link: https://onlinecourses.nptel.ac.in/noc24_cs94/preview
2. NPTEL Course: Digital Forensic , By Dr. Navjot Kaur Kanwal | Dr. Harisingh Gour Vishwavidyalaya, Sagar (M.P.) Department of Criminology and Forensic Science Web Link: https://onlinecourses.swayam2.ac.in/cec20_lb06/preview
3. NPTEL Course: INTRODUCTION TO CYBER SECURITY By Dr. Jeetendra Pande | Uttarakhand Open University, Haldwani Web Link: https://onlinecourses.swayam2.ac.in/nou19_cs08/preview
4. Nptel Course:Cyber Crime AdministrationBy Adv. Jayashree Nangare | Savitribai Phule Pune University Web Link: https://onlinecourses.swayam2.ac.in/cec22_lw07/preview

A. IN-SEMESTER ASSESSMENT (50 MARKS)

1. Continuous Assessment (20 Marks)

Suggested breakup of distribution

a. Assignment on live problems/ case studies, wherein problems are given prior. Students are expected to research and collect required resources. They can use the resources and solve the problem on assigned date and time in Institute premises in presence of faculty member. : 10 Marks
b. Flip classroom: 05 Marks
c. Observation and active participation in class :05 Marks

2. Mid Semester Exam (30 Marks)

Mid semester examination will be based on 40% to 50% syllabus

B. END SEMESTER EXAM (50 MARKS)

End Semester Examination will be based on syllabus coverage up to the Mid Semester Examination (MSE) carrying 20% to 30% weightage, and the syllabus covered from MSE to ESE carrying 70% to 80% weightage.

Course Type	Course Code	Course Name	Credits
HMC	HMCCS602	INFRASTRUCTURE SECURITY	03

Examination Scheme					
Distribution of Marks			Exam Duration (Hrs.)		Total Marks
In-semester Assessment		End Semester Examination (ESE)			
Continuous Assessment	Mid-Semester Exam (MSE)		MSE	ESE	
20	30	50	1.5	2	100

Pre-requisite:

NIL

Program Outcomes addressed:

1. PO1: Engineering knowledge
2. PO2: Problem analysis
3. PO3:Design/development of solutions
4. PO4:Conduct investigations of complex problems
5. PO5: Engineering tool usage
6. PO 6: The Engineer and The World
7. PO 7: Ethics
8. PO 11: Life-long learning

Course Objectives:

1. To make learner recall the basics to protect critical information assets through effective controls and monitoring.
2. Guide learner to Identify, analyse, prevent, and mitigate software vulnerabilities and malware threats.
3. Assist learner to illustrate Securing mobile devices and wireless networks against contemporary security threats.
4. Assist learner to investigate cloud infrastructure vulnerabilities and their countermeasures
5. To assist learner to learn the different attacks on Open Web Applications and Web services.
6. To equip students with the knowledge and skills required for modern security architectures and learn how to automate and orchestrate security processes effectively.

Module	Details	Hrs.
00.	**Course Introduction** The Infrastructure Security course provides a comprehensive understanding of cybersecurity fundamentals. Covering cyber-attacks, authentication methods, software vulnerabilities, and access control models, students learn to safeguard digital infrastructure. Topics include	01

	database security, wireless LAN security, cloud security and web security.	
01.	**Information Asset Security and Control** ***Learning Objective:*** *To make learner understand the importance of information assets and the deployment o managerial, technical, and physical controls for physical access and environmenta security..*	**08-10**
	Contents: Information Assets and its importance, Physical Access and Environmental Controls: Managerial, Technical and Physical Controls, Control Monitoring and Effectiveness, Environmental Exposures and Controls, Physical Access Exposures and Controls, Identity and Access Management: Logon IDs and Passwords System Access Permission, Biometric, SSO, Access Control Policies and Models (DAC,MAC, RBAC, ABAC, BIBA, Bell La Padula), Information Security and External Parties. **Demonstration of Password Management and Access Control.**	
	Self-Learning Topics: *Authentication and Access Control Services- RADIUS, TACACS, and TACACS+*	
	Learning Outcomes: *A learner will be able to* *LO 1.1: Apply engineering fundamentals to analyze and implement access control models such as RBAC, MAC, and ABAC. (P.I.-1.3.1)* *LO 1.2: Apply the theory and principles of cybersecurity to solve security challenges in physical environments. (P.I.-1.4.1)* *LO 1.3: Identify processes and parameters for mitigating unauthorized access to information assets and describe engineering roles related to ensuring public security and data protection in information asset management.. (P.I.-2.1.2), (P.I.-6.1.1)* *LO 1.4: Analyze functionalities required for defending against threats and how Understand the impact of different threats on public safety and critical infrastructures (P.I.-2.4.2), (P.I.-6.3.1)* *LO 1.5: Identify modern engineering tools, techniques, and resources required for securing information assets. (P.I.-5.1.1)* *LO 1.6: Identify strengths and limitations of discipline-specific tools such as malware analysis frameworks, penetration testing tools, and vulnerability scanners. (P.I.-5.2.1)*	
02.	**Software Security** ***Learning Objective:*** *To make learner derive and demonstrate the representation of different types of software vulnerabilities. Also expected to apply the concept of software security at different level of software.*	**07-09**
	Contents: Software Vulnerabilities: Buffer overflow, Format String, Cross-Site Scripting, SQL Injection, Types of Malware Operating System Security: Memory and Address Protection, File Protection Mechanism, User Authentication. Database Security: Database Security Requirements, Reliability and Integrity, Sensitive Data, Inference Attacks, Multilevel Database Security	

	Demonstration of Malware attacks	
	Self-Learning Topics: *Format String, File System Security (Windows and Linux OS)*	
	Learning Outcomes: *A learner will be able to* *LO 2.1: Identify functionalities and computing resources required to prevent different types of malware and software vulnerabilities and evaluate malware security solutions in the context of public safety and legal requirements. (P.I.-2.2.2), (P.I.-6.1.1)* *LO 2.2: Identify processes and parameters for mitigating vulnerabilities in software applications and Recognize and analyze emerging trends in software security threats and the need for continuous learning. (P.I.-2.1.2), (P.I.-11.2.2)* *LO 2.3: Use appropriate tools and techniques to collect and analyze cyber threat intelligence data related to software security. (P.I.-4.3.1)* *LO 2.4: Demonstrate an ability to analyze software vulnerabilities and propose appropriate countermeasures. (P.I.-4.3.2)* *LO 2.5: Identify and compare security tools for Malware security, evaluating their strengths and limitations. (P.I.-5.3.1)* *LO 2.6: Identify strengths and limitations of vulnerability analysis and penetration testing tools for software security. (P.I.-5.2.1)* *LO 2.7: Identify the relationship between security risks and societal security concerns in software applications. (P.I.-6.3.2)* *LO 2.8: Analyze sourced technical literature to evaluate security frameworks and their applicability in modern software security. (P.I.-2.4.2) (P.I.-11.3.2)*	
03.	**Wireless Security** ***Learning Objective:*** *To make learner is understand mobile device security, encompassing wireless threat mitigation and device security considering different wireless infrastructures.*	**06-08**
	Contents: Mobile Device Security- Wireless Security Threats and Risk Mitigation, Device Security, IEEE 802.11xWireless LAN Security, VPN Security, Wireless Intrusion Detection System (WIDS), Public Global Internet Infrastructure, Internet of Things **Demonstration of wireless security tools**	
	Self-Learning Topics: *Wireshark, Cain and Abel, Aircrack.*	
	Learning Outcomes: *A learner will be able to* *LO 3.1: Apply engineering fundamentals to secure wireless communication based applications and Analyze the risks of wireless security breaches and their societal impact. (P.I.-1.3.1), (P.I.-6.3.2)* *LO 3.2: Apply security principles to solve security challenges such as IEEE 802.11xWireless LAN and data protection and Evaluate wireless security threats and their effect on privacy and public safety. (P.I.-1.4.1), (P.I.-6.1.1)* *LO 3.3: Explore and synthesize system requirements for securing cloud-based infrastructure using modern security models. (P.I.-3.1.5)* *LO 3.4: Perform systematic evaluation of different VPN security solutions. (P.I.-3.3.1)*	

	LO 3.5: Identify and assess modern security tools required for securing wireless environments. (P.I.-5.1.1) *LO 3.6: Identify strengths and limitations of Wireless Intrusion Detection System (WIDS). (P.I.-5.2.1)*	
04.	**Cloud Security** ***Learning Objectives:*** *To make learner iillustrate cloud security risks and effective countermeasures, ensuring proficiency in data protection, cloud application security, cloud identity and access management, and the implementation of cloud security services to safeguard cloud-based infrastructures.* **Contents:** Cloud Security Risks and Countermeasures, Data Protection in Cloud, Cloud Application Security, Cloud Identity and Access Management, Cloud Security as a Service. **Implementation of Security as a Service (SECaaS)** ***Self-Learning Topics:*** *Metasploit, Ettercap* ***Learning Outcomes:*** *A learner will be able to* *LO 4.1: Apply engineering fundamentals to secure cloud-based security applications and Analyze the risks of cloud security breaches and their societal impact. (P.I.-1.3.1), (P.I.-6.3.2)* *LO 4.2: Apply security principles to solve cloud security challenges such as IAM and data protection and Evaluate cloud threats and their effect on privacy and public safety. (P.I.-1.4.1), (P.I.-6.1.1)* *LO 4.3: Explore and synthesize system requirements for securing cloud-based infrastructure using modern security models. (P.I.-3.1.5)* *LO 4.4: Perform systematic evaluation on cloud security solutions. (P.I.-3.3.1)* *LO 4.5: Identify and assess modern security tools required for securing cloud environments. (P.I.-5.1.1)* *LO 4.6: Identify strengths and limitations of cloud security posture management (CSPM) tools. (P.I.-5.2.1)*	**05-07**
05.	**Web Security** ***Learning Objective/s:*** *Learner is expected to recall and interpret comprehensive web security considerations including user authentication, session management, encryption protocols, privacy concerns, defense against web browser attacks, prevention of common threats* **Contents:** Web Security Considerations, User Authentication and Session Management, Cookies, SSL, HTTPS, SSH, Privacy on Web, Web Browser Attacks, Account Harvesting, Web Bugs, Clickjacking, Cross-Site Request Forgery, Session Hijacking and Management, Phishing and Pharming Techniques, DNS Attacks, Web Service Security, Secure Electronic Transaction, Email Attacks, Web Server Security as per OWASP, Firewalls. **Demonstration of different web attacks.** ***Self-Learning Topics:***	**08-10**

	Penetration Testing tools: SQL Map, Wapiti.	
	Learning Outcomes :	
	A learner will be able to *LO 5.1: Identify processes and techniques to prevent Web attacks and ethical concerns related to web application security and responsible disclosure. (P.I.-2.1.2), (P.I.-7.1.1)* *LO 5.2: Analyze the effectiveness of Security mechanisms in preventing web security threats and analyze industry trends and research new security solutions for web-based applications.. (P.I.-2.4.2), (P.I.-11.3.2)* *LO 5.3: Use security tools to analyze web application vulnerabilities such as SQL injection and XSS. (P.I.-4.3.1)* *LO 5.4: Demonstrate an ability to evaluate and mitigate risks in web services. (P.I.-4.3.2)* *LO 5.5: Create and apply penetration testing techniques for enhancing web security. (P.I.-5.1.2)* *LO 5.6: identify strengths and limitations Secure Electronic Transaction for web security. (P.I.-5.2.1)* *LO 5.7: Examine the role of ethical hacking in improving web security practices. (P.I.-7.2.1)* *LO 5.8: Identify and study need of OWASP through continuous learning. (P.I.-11.2.1)*	
06.	*Recent advancements in Infrastructure Security*	**03-05**
	Learning Objective/s: *To make learner apply the knowledge and skills required to navigate and analyse rapidly evolving landscape of Infrastructure security and its applications in contemporary technology.*	
	Contents: Zero Trust Architecture, Cyber Threat Intelligence, Cloud Security Posture Management (CSPM), Container Security and Kubernetes Security, Identity and Access Management (IAM) Innovations, Automation and Orchestration. **Demonstration of Real Time Threat Intelligence using latest tools.**	
	Self-Learning Topics: *Software-Defined Networking (SDN) for Agile and Scalable Infrastructure Management.*	
	Learning Outcomes:	
	A learner will be able to *LO 6.1: Select and implement container security techniques to secure infrastructure. (P.I.-3.1.5)* *LO 6.2: Systematically evaluate Zero Trust Architecture as a model for enterprise security. (P.I.-3.3.1)* *LO 6.3: Identify and demonstrate modern security tools used for securing cloud and enterprise infrastructure. (P.I.-5.1.1)* *LO 6.4: identify strengths and limitations of automation and orchestration tools for security operations. (P.I.-5.2.1)* *LO 6.5: Examine the ethical considerations related to infrastructure security and responsible AI, and explain how cybersecurity principles can be applied to mitigate ethical risks. (P.I.-1.4.1) (P.I.-7.2.1)*	

	LO 6.6: Analyze ethical dilemmas in infrastructure security concerning user privacy and surveillance. Identify key processes and parameters used to mitigate these challenges. (P.I.-2.1.2) (P.I.-7.1.1) *LO 6.7: Investigate emerging technologies in infrastructure security. Understand how do engineering fundamentals support the development of new security models to address evolving threats. (P.I.-1.3.1) (P.I.-11.2.2)* *LO 6.8: Review industry best practices for securing modern infrastructure. Understand computing resources and security functionalities are required to prevent modern cyber threats. (P.I.-2.2.2) (P.I.-11.3.2)*	
	Course Conclusion	**01**
	Total	**45**

Performance Indicators:

P.I. No.	P.I. Statement
1.3.1	Apply engineering fundamentals
1.4.1	Apply theory and principles of computer science engineering to solve an engineering problem
2.1.2	Identifies processes/modules/algorithms of a computer based system and parameters to solve a problem
2.2.2	Identifies functionalities and computing resources
2.4.2	Analyze and interpret the results using contemporary tools.
3.1.5	Explore and synthesize system requirements from larger social and professional concerns.
3.3.1	Ability to perform systematic evaluation of the degree to which several design concepts meet the criteria.
4.3.1	Use appropriate procedures, tools and techniques to collect and analyze data
4.3.2	Critically analyze data for trends and correlations, stating possible errors and limitations
5.1.1	Identify modern engineering tools, techniques and resources for engineering activities
5.1.2	Create/adapt/modify/extend tools and techniques to solve engineering problems
5.2.1	Identify the strengths and limitations of tools for (i) acquiring information, (ii) modeling and simulating, (iii) monitoring system performance, and (iv) creating engineering designs
5.3.1	Discuss limitations and validate tools, techniques and resources
6.1.1	Identify and describe various engineering roles; particularly as pertains to protection of the public and public interest at global, regional and local level
6.3.1	Identify risks/impacts in the life-cycle of an engineering product or activity
6.3.2	Understand the relationship between the technical, socio economic and environmental dimensions of sustainability
7.1.1	Identify situations of unethical professional conduct and propose ethical alternatives
7.2.1	Identify tenets of the ASME professional code of ethics
11.2.2	Recognize the need and be able to clearly explain why it is vitally important to keep current regarding new developments in your field
11.3.2	Analyze sourced technical and popular information for feasibility, viability,sustainability, etc.

Course Outcomes: A learner will be able to -

CO ID	Course Outcome
1	Apply cybersecurity principles to analyze access control models on secure infrastructure, identify security tools, and evaluate threats to public safety and infrastructure while identifying their strengths and limitations. (LO 1.1, LO 1.2, LO 1.3, LO 1.4, LO 1.5, LO 1.6)
2	Investigate security strategies by identifying different tools for analyzing software vulnerabilities and security threats in databases and operating systems while evaluating

malware security solutions in the context of public safety and emerging trends. (LO 2.1, LO 2.2, LO 2.3, LO 2.4, LO 2.5, LO 2.6, LO 2.7, LO 2.8)

3 Identify functionalities and security techniques to analyze and mitigate risks in cloud and wireless environments while evaluating software security solutions, emerging trends, and security frameworks through continuous learning. (LO 3.1, LO 3.2, LO 3.3, LO 3.4, LO 3.5, LO 3.6, LO 4.1, LO 4.2, LO 4.3, LO 4.4, LO 4.5, LO 4.6)

4 Analyze various web security threats by identifying security tools and techniques to evaluate and mitigate risks in web applications while applying ethical principles and industry best practices. (LO 5.1, LO 5.2, LO 5.3, LO 5.4, LO 5.5, LO 5.6, LO 5.7, LO 5.8)

5 Investigate emerging technologies and review industry frameworks to ensure continuous improvement in securing enterprise environments while identifying strengths and limitations of modern security, automation, and orchestration tools. (LO 6.1, LO 6.2, LO 6.3, LO 6.4, LO 6.5, LO 6.6, LO 6.7, LO 6.8)

CO-PO Mapping Table with Correlation Level

CO ID	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
HMCCS602.1	3	3	-	-	3	3	-	-	-	-	-
HMCCS602.2	-	3	-	3	3	3	-	-	-	-	3
HMCCS602.3	3	-	3	-	3	3	-	-	-	-	-
HMCCS602.4	-	3	-	3	3	-	3	-	-	-	3
HMCCS602.5	3	3	3	-	3	-	3	-	-	-	3
Average	**3**	**3**	**3**	**3**	**3**	**3**	**3**	-	-	-	**3**

Text Books :

1. Computer Security Principles and Practice, William Stallings, Seventh Edition, 2017, Pearson Education
2. Security in Computing, Charles P. Pfleeger, Fifth Edition, 20011, Pearson Education
3. Network Security and Cryptography, Bernard Menezes, First Edition,1 April 2010, Cengage Learning
4. Network Security Bible, Eric Cole, Second Edition, 31 March 2011, Wiley Publication

Reference Books :

1. Web Application Hackers Handbook, by Dafydd Stuttard, Marcus Pinto, 2nd Edition, 31 August 2011, Wile Publication
2. Computer Security, Dieter Gollman, Third Edition, 1 January 2014, Wiley Publication

Other Resources :

1. NPTEL Course: Systems and Usable Security, Prof. Neminath Hubballi, Department of Computer Science and Engineering, IIT Guwahati, Web link- https:// https://nptel.ac.in/courses/106/106/106106234/

2. NPTEL Course: Hardware Security By Prof. Debdeep Mukhopadhyay, Department of Computer Science and Engineering, IIT-Kharagpur, Web link- https:// nptel.ac.in/courses/106/105/106105194/

A. IN-SEMESTER ASSESSMENT (50 MARKS)

1. Continuous Assessment (20 Marks)

Suggested breakup of distribution

a. One MCQ Test as per GATE exam pattern / level: 05 Marks
b. One Class Test:05 Marks
c. One Open Notes Test: 05 Marks
d. Regularity and active participation :05 Marks

2. Mid Semester Examination (30 Marks)

Mid semester examination will be based on 40% to 50% syllabus.

B. END SEMESTER EXAMINATION (50 MARKS)

End Semester Examination will be based on syllabus coverage up to the Mid Semester Examination (MSE) carrying 20% to 30% weightage, and the syllabus covered from MSE to ESE carrying 70% to 80% weightage.

Course Type	Course Code	Course Name	Credits
HMC	HMCCS703	SECURITY AUDIT AND RISK ASSESSMENT	04

Examination Scheme					
Distribution of Marks			Exam Duration (Hrs.)		Total Marks
In-semester Assessment		End Semester Exam (ESE)			
Continuous Assessment	Mid-Semester Exam (MSE)		MSE	ESE	
20	30	50	1.5	2	100

Pre-requisite :

1. HMCCS501 : CYBERCRIME AND CYBERSECURITY
2. HMCCS602 : INFRASTRUCTURE SECURITY

Program Outcomes addressed :

1. PO1: Engineering knowledge
2. PO2: Problem analysis
3. PO3:Design/development of solutions
4. PO4:Conduct investigations of complex problems
5. PO5:Modern tool usage
6. PO 6: The Engineer and The World
7. PO 7: Ethics
8. PO 8: Individual and team work
9. PO 9: Communication
10. PO10: Project management and finance
11. PO 11: Life-long learning

Course Objectives :

1. To enable learners to recall the fundamentals of Information System (IS) auditing, including audit purpose, professional ethics, and the complete audit life cycle for evaluating information security effectiveness.
2. To familiarize learners with IT governance frameworks, standards, and regulatory requirements essential for maintaining compliance and organizational accountability.
3. To develop the ability to manage IT infrastructure lifecycles through effective project management and incident management practices that enhance operational efficiency and service quality.
4. To cultivate analytical skills in identifying, assessing, and mitigating security risks using both qualitative and quantitative risk assessment methods for informed security decision-making.
5. To equip learners with the competence to design, perform, and report information security audits, including risk-based planning, evidence evaluation, and follow-up actions in alignment with professional ethics.
6. To enhance practical understanding through real-world case studies and applications involving audits of IT infrastructure, networks, cloud environments, and mobile systems using modern tools and techniques.

Module	Details	Hrs
00.	**Course Introduction**	01

	This course provides learners with comprehensive knowledge of auditing principles, IT governance frameworks, and risk management practices essential for ensuring information system security. Through real-world case studies, learners develop the skills to conduct effective security audits, identify vulnerabilities, and recommend improvements for organizational resilience.	
01.	**Introduction to IT Audit and Security** ***Learning Objective/s:*** *To make learner understand the purpose and importance of IS audits, auditor ethics, and key skills required for effective auditing, along with the audit life cycle, reporting, and post-audit activities.*	**10-12**
	Contents: Understanding the Demand for IS Audits, Professional ethics for auditor, Purpose of an Audit, Skills and Knowledge Required to Be an IS Auditor, The Auditing Life Cycle, understanding corporate organizational structure, Pre-audit checklist, Information Gathering, Internal and External Security Audit, Information Security Audit Deliverables & Writing Report, Result Analysis, Post Auditing Actions, Report Retention etc.	
	Self-Learning Topics: *components of ISMS and conceptual framework* ***Learning Outcomes:*** *A learner will be able to* 1. ***LO 1.1:*** *Apply auditing fundamentals to identify the demand, purpose, and ethics of IS audits, and evaluate their role in ensuring responsible professional practice. (P.I.-1.4.1, 7.2.2)* 2. ***LO 1.2:*** *Apply the auditing life cycle to the corporate infrastructure to prepare structured audit reports demonstrating clear professional communication. (P.I.-1.3.1, 9.1.2)* 3. ***LO 1.3****: Identify and articulate the problem, scope, and objectives of an Information Security audit, and deliver effective oral presentations of audit and business rationale to both technical and non-technical audiences. (P.I.-4.1.1, 9.2.2)* 4. ***LO 1.4****: Choose appropriate audit procedures to assess information systems while adhering to professional codes of ethics and ensuring integrity in audit practices. (P.I.-4.1.2, 7.2.1)*	
02.	**IT Governance and Standards** ***Learning Objective/s:*** *To make learner analyze various IT governance frameworks and standards like COSO, COBIT, ITIL, and ISO 27001, along with key regulations and acts governing internal controls and data privacy in organizations.*	**7-9**
	Contents: Frameworks and Standards: Introduction to Internal IT Controls, Frameworks, and Standards, COSO, COBIT, ITIL, ISO 27001. Regulations:	

	An Introduction to Legislation Related to Internal Controls, The Sarbanes-Oxley Act of 2002, Gramm-Leach-Bliley Act, Privacy Regulations, Health Insurance Portability and Accountability Act of 1996, EU Commission and Basel II, Payment Card Industry (PCI), HIPPA.	
	Self-Learning Topics: *NIST Cybersecurity Framework* ***Learning Outcomes :*** *A learner will be able to* 1. ***LO 2.1****: Identify processes and parameters for evaluating internal IT control systems and interpret how governance frameworks align with legislation and public protection standards. (P.I.-2.1.2, 6.1.1)* 2. ***LO 2.2****: Compare and contrast IT governance frameworks such as COBIT, COSO, and ITIL to select the most effective method for ensuring compliance, while analyzing their contribution to sustainable and ethical IT practices. (P.I.-2.2.4, 6.3.2)* 3. ***LO 2.3****: Select and apply suitable quality attributes defined by ISO/IEC/IEEE standards to design a compliant IT governance model, demonstrating adherence to professional ethical codes and accountability principles. (P.I.-3.1.4, 7.2.1)* 4. ***LO 2.4****: Evaluate multiple governance framework implementations to determine the most effective design for meeting security and compliance objectives, and examine ethical implications in governance implementation. (P.I.-3.3.1, 7.2.2)* 5. ***LO 2.5****: Identify and use modern engineering tools for auditing and monitoring compliance with IT standards like ISO 27001, while recognizing the importance of continuous professional learning and updating technical skills. (P.I.-5.1.1, 11.2.2)* 6. ***LO 2.6****: Assess the strengths and limitations of compliance and governance tools, identifying knowledge gaps and demonstrating self-directed learning to adapt to evolving IT standards and regulatory frameworks. (P.I.-5.2.1, 11.1.2)*	
03.	**Infrastructure Lifecycle Management and IT Operations, Maintenance, and Support** ***Learning Objective/s:*** *To make learner illustrate project management practices, software development methodologies, and IT service management processes including configuration, release, capacity, and incident management for effective IT operations and system maintenance.*	**9-11**
	Contents: Project management practices, Methodology and tools for software, development, Configuration and releases management, Data migration and information systems, implementation, Goals and practices of system launch quality assessment. Practices in IT services management and operational management, Planning and capacity management, Problems and incidents management.	
	Self-Learning Topics: *Disaster recovery planning and plans testing.* ***Learning Outcomes :***	

	A learner will be able to 1. ***LO 3.1****: Identify and analyze IT processes, dependencies, and parameters for configuration and release management, and plan project tasks and resources required for successful IT infrastructure implementation. (P.I.-2.1.2, 10.3.1)* 2. ***LO 3.2****: Compare and evaluate alternative operational and capacity management methods for a given IT infrastructure, and apply project management tools to monitor IT support activities efficiently. (P.I.-2.2.4, 10.3.2)* 3. ***LO 3.3****: Select and apply appropriate quality attributes and design practices to ensure reliability, scalability, and maintainability in IT system implementation. (P.I.-3.1.4)* 5. ***LO 3.4:*** *Perform systematic evaluation of IT service management frameworks to assess their effectiveness in improving operational performance.* ***(****P.I.-3.3.1)* 4. ***LO 3.5****: Identify and utilize modern engineering tools required for configuration, release, and incident management in IT operations. (P.I.-5.1.1)* 5. ***LO 3.6****: Analyze the strengths and limitations of tools used for configuration tracking, problem management, and service optimization.(P.I.-5.2.1)*	
04.	**Security Risk Assessment and Analysis** ***Learning Objective/s:*** *To make learner understand the concepts and processes of IT risk management, including risk identification, assessment, mitigation, and reporting, to ensure effective security risk analysis and informed decision-making.*	**9-11**
	Contents: Benefits of Risk Management, Risk Management from an Executive Perspective, IT Risk Management Life Cycle, Security **Risk Assessment**: Introduce the Team, review business mission, Identify critical system, Asset classes, identifying threats, Quantitative Risk Analysis, Qualitative Risk Analysis, Security Risk mitigation, Security Risk assessment Reporting.	
	Self-Learning Topics: *RIIOT method and approaches.* ***Learning Outcomes :*** *A learner will be able to* 1. ***LO 4.1:*** *Apply engineering fundamentals to secure information systems and analyze the risks of security breaches and their societal impact. (P.I.-1.3.1, 6.3.2)* 2. ***LO 4.2:*** *Apply the theory and principles of information security risk management to identify and assess critical systems, while interpreting relevant legislation and professional responsibilities to ensure public protection and organizational compliance. (P.I.-1.4.1, 6.1.1)* 3. ***LO 4.3:*** *Critically analyze risk data to identify trends in threats and vulnerabilities, stating the limitations and potential errors in the qualitative/quantitative analysis.(P.I. - 4.3.2)* 4. ***LO 4.4:*** *Synthesize information from various risk analysis steps to reach a valid, overarching conclusion about the organization's risk posture and priority areas. (P.I. - 4.3.4)* 5. ***LO 4.5:*** *Perform a systematic evaluation of different risk mitigation controls against criteria like cost, effectiveness, and operational impact to select an optimal strategy.(P.I. - 3.3.1)*	

	6. ***LO 4.6:*** *Explore alternative risk treatment strategies (avoid, transfer, mitigate, accept) for a given set of high-risk findings.(P.I. - 3.2.1)*	
05.	**Information Security Audit** ***Learning Objective/s:*** *To make learner recall and interpret the complete audit process including audit planning, risk assessment, evidence collection, reporting of findings, and follow-up actions for effective information security auditing.* **Contents:** The Audit Program, Establishing and Approving an Audit Charter, Preplanning Specific Audits, Performing an Audit Risk Assessment, Determining Whether an Audit Is Possible, Performing the Audit, Gathering Audit Evidence, Conducting Audit Evidence Testing, Generating Audit Findings, Report Findings, Conducting Follow-up. ***Self-Learning Topics:*** *Perpetration of audit charter for e commerce company.* ***Learning Outcomes :*** *A learner will be able to* 1. ***LO 5.1:*** *Compare and evaluate alternative audit methodologies to select the most effective approach for conducting security audits, while applying moral and ethical principles to ensure integrity and accountability in audit practices. (P.I.-2.2.4, 7.2.2)* 2. ***LO 5.1****: Develop and execute an information security audit plan, applying research-based audit procedures while demonstrating teamwork norms to achieve defined goals. (P.I.-4.2.1, 8.1.2)* 3. ***LO 5.2:*** *Analyze and evaluate audit evidence collaboratively, applying problem-solving and leadership skills to resolve audit-related conflicts. (P.I.-4.3.2, 8.2.1)* 4. ***LO 5.3:*** *Analyze audit results and propose actionable improvements that ensure compliance with professional ethics and organizational policies. (P.I.-2.4.4, 7.2.1,)* 5. ***LO 5.4****: Develop and justify evidence-based audit procedures by analyzing technical configurations and organizational contexts to verify control objectives.* *(P.I.-4.1.2, 9.1.1)*	**11-13**
06.	**Practical Applications and Case Studies** ***Learning Objective/s:*** *To make learner apply practical auditing techniques for network devices, operating systems, web applications, databases, and cloud environments through real-world case studies and applications.* **Contents:** Auditing Routers, Switches, and Firewalls, Auditing Unix and Linux Operating Systems, Auditing Web Servers and Web Applications, Auditing Databases, Auditing WLAN and Mobile Devices, IT Infrastructure Audit case study, Cloud Application Security Audit, Case Study of FDIC's Cloud Computing Environment. ***Self-Learning Topics:*** *Auditing Virtualized Environments.* ***Learning Outcomes :***	**6-8**

	A learner will be able to 1. ***LO 6.1:*** *Determine auditing tools and techniques to assess the security of routers, servers, and databases, and analyze their compliance with industry standards. (P.I.-5.1.1, 6.2.1)* 2. ***LO 6.2:*** *Identify processes and parameters for auditing network devices, operating systems, and applications, and effectively present audit findings to technical and non-technical audiences through clear oral communication. (P.I.-2.1.2, 9.2.2)* 3. ***LO 6.3:*** *Demonstrate cloud, WLAN, and mobile security audits and analyze their implications for privacy and sustainability. (P.I.-4.3.2, 6.3.2)* 4. ***LO 6.4****: Develop and justify systematic testing procedures to validate implemented security controls and investigate emerging technologies to address knowledge gaps in evolving security domains. (P.I.-4.1.2, 11.1.2)* 5. ***LO 6.5:****Explore and research emerging tools for auditing virtualized and cloud environments, and adapt to evolving technologies. (P.I.-11.2.2, 5.1.2)*	
	Course Conclusion	**01**
Total		**60**

Course Outcomes: A learner will be able to -

CO ID	Course Outcome
HMCCS703.1	Apply auditing fundamentals to understand IS audit demand, ethics, and professional practices; analyze the audit life cycle; and communicate audit scope and objectives effectively to diverse stakeholders. (LO 1.1, LO 1.2, LO 1.3, LO 1.4)
HMCCS703.2	Analyze IT governance frameworks and legal regulations (COBIT, ITIL, ISO 27001, SOX, HIPAA), evaluate their societal impact, and synthesize emerging standards to ensure compliant and sustainable IT governance. (LO 2.1, LO 2.2, LO 2.3, LO 2.4, LO 2.5, LO 2.6)
HMCCS703.3	Apply project management principles, configuration and release management, and IT service processes to improve operational efficiency, ensure sustainability, and validate system performance using modern tools. (LO 3.1, LO 3.2, LO 3.3, LO 3.4, LO 3.5, LO 3.6)
HMCCS703.4	Apply engineering fundamentals to assess security risks, analyze and synthesize risk data, evaluate mitigation strategies, and explore alternative treatments to strengthen organizational risk posture. (LO 4.1, LO 4.2, LO 4.3, LO 4.4, LO 4.5, LO 4.6)
HMCCS703.5	Develop and execute information security audits, analyze evidence, and propose ethical improvements; assess real-world infrastructure audits (routers, servers, cloud, mobile) using modern tools and continuous learning approaches. (LO 5.1, LO 5.2, LO 5.3, LO 5.4, LO 6.1, LO 6.2, LO 6.3, LO 6.4, LO 6.5)

CO-PO Mapping Table with Correlation Level

CO ID	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
HMCCS703.1	3			3			3		3		
HMCCS703.2		3	3		3	3	3				3
HMCCS703.3		3	3		3					3	
HMCCS703.4	3		3	3		3					
HMCCS703.5		3		3	3	3	3	3	3		3
Average	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**

Performance Indicators:

P.I. No.	P.I. Statement
1.3.1	Apply engineering fundamentals.
1.4.1	Apply theory and principles of computer science engineering to solve an engineering problem.
2.1.2	Identifies processes/modules/algorithms of a computer-based system and parameters to solve a problem.
2.2.4	Compare and contrast alternative solution/methods to select the best methods.
2.4.4	Arrive at conclusions with respect to the objectives.
3.1.4	Ability to choose appropriate quality attributes as defined by ISO/IEC/IEEE standard.
3.2.1	Ability to explore design alternatives.
3.3.1	Ability to perform systematic evaluation of the degree to which several design concepts meet the criteria.
4.1.1	Define a problem for purposes of investigation, its scope and importance.
4.1.2	Ability to choose appropriate procedure/algorithm, dataset and test cases.
4.2.1	Design and develop appropriate procedures/methodologies based on the study objectives.
4.3.2	Critically analyze data for trends and correlations, stating possible errors and limitations.
4.3.4	Synthesize information and knowledge about the problem from the raw data to reach appropriate conclusions.
5.1.1	Identify modern engineering tools, techniques and resources for engineering activities.
5.1.2	Create/adapt/modify/extend tools and techniques to solve engineering problems.
5.2.1	Identify the strengths and limitations of tools for acquiring information, modeling, simulating, monitoring system performance, and creating designs.
6.1.1	Identify and describe various engineering roles, particularly as pertains to protection of the public and public interest at global, regional and local levels.
6.2.1	Interpret legislation, regulations, codes, and standards relevant to your discipline and explain their contribution to the protection of the public.
6.3.2	Understand the relationship between the technical, socio-economic and environmental dimensions of sustainability.
7.2.1	Identify tenets of the professional code of ethics.
7.2.2	Examine and apply moral and ethical principles to known case studies.
8.1.2	Implement the norms of practice (rules, roles, charters, agendas, etc.) of effective teamwork to accomplish a goal.
8.2.1	Demonstrate effective communication, problem solving, conflict resolution and leadership skills.
9.1.1	Read, understand and interpret technical and non-technical information.
9.1.2	Produce clear, well-constructed, and well-supported written engineering documents.
9.2.2	Deliver effective oral presentations to technical and non-technical audiences.
10.3.1	Identify the tasks required to complete an engineering activity, and the resources required to complete the tasks.
10.3.2	Use project management tools to schedule an engineering project so it is completed on time and on budget.
11.1.2	Identify deficiencies or gaps in knowledge and demonstrate an ability to source information to close this gap.
11.2.2	Recognize the need and be able to clearly explain why it is vitally important to keep current regarding new developments in your field.

Text Books :

1. Internal Auditing & Information Systems Auditing- Comprehensive Guide for Digital Era, V Venkataraman And Ca N Sankara Narayana Pillai, 2016, CCH publication

2. Certified Information Systems Auditor (CISA) Cert Guide, Michael Gregg, Rob Johnson 2018, Pearson Education

3. The Security Risk Assessment Handbook, Douglas J. Landoll, 1st edition, 2021, CRC press

4. IT Auditing: Using Controls to Protect Information Assets, Chris Davis, Mike Schiller with Kevin Wheeler 2nd Edition, 2011, McGraw Hill

Reference Books :

1. Information Technology Control and Audit, Angel R. Otero, Fifth Edition, 2018, CRC Press

2. CISA Certified Information Systems Auditor All-in-One Exam Guide, Peter H. Gregory, Fourth Edition, 2019, McGraw Hill LLC

Other Resources :

1. NPTEL Course: Introduction to Information Security – I, Prof. V. Kamakoti, Prof. Dilip H Ayyar, Department of Computer Science, IIT Madras Web link- https://nptel.ac.in/courses/106106129

2. NPTEL Course: Cyber Security and Privacy, Prof. Saji K Mathew, Department of management studies, IIT Madras, Web link- https://nptel.ac.in/courses/106106248

IN-SEMESTER ASSESSMENT (50 MARKS)

Continuous Assessment (20 Marks)

Suggested breakup of distribution

A. One MCQ Test as per GATE exam pattern / level: 05 Marks
B. One Class Test: 05 Marks
C. Mind map activity: 05 Mars
D. Regularity and active participation in class : 05 Marks

Mid Semester Examination (30 Marks)

Mid semester examination will be based on 40% to 50% syllabus.

END SEMESTER EXAMINATION (50 MARKS)

End Semester Examination will be based on syllabus coverage up to the Mid Semester Examination (MSE) carrying 20% to 30% weightage, and the syllabus covered from MSE to ESE carrying 70% to 80% weightage.

Course Type	Course Code	Course Name	Credits
HML	HMLCS701	CYBERSECURITY LABORATORY	02

Examination Scheme					
Distribution of Marks			Exam Duration (Hrs.)		Total Marks
In-semester Assessment		End Semester Exam (ESE)			
Continuous Assessment	Mid-Semester Exam (MSE)		MSE	ESE	
50	--	--	--	--	50

Pre-requisite:

1. HMCCS501: Cybercrime & Cyber Security
2. HMCCS602: Infrastructure Security
3. HMCCS703 :Security Audit & Risk Assessment

Program Outcomes addressed:

1. PO1: Engineering knowledge
2. PO2:Problem analysis
3. PO3:Design/Development of Solutions
4. PO4:Conduct investigations of complex problems
5. PO5:Engineering tool usage
6. PO7:Ethics
7. PO8:Individual and team work
8. PO9:Communication
9. PO10:Project management and finance
10. PO11:Life-long learning

Course Objectives:

1. To acquaint students with fundamental network security concepts and practices for identifying vulnerabilities and examining network traffic to uncover potential threats.
2. To introduce students to cryptographic methods for securing communications and evaluating encryption mechanisms that uphold data integrity and confidentiality.
3. To engage students in ethical hacking frameworks and techniques for assessing and validating vulnerabilities within networks and applications.
4. To equip students with the knowledge and skills to implement effective endpoint protection strategies that defend systems from malware and unauthorized access.
5. To enable students to comprehend and interpret cyber incident responses and forensic investigation procedures for determining root causes and assessing impacts.
6. To orient students toward the application of monitoring, risk assessment, and security management methodologies for sustaining and improving organizational security posture.

Module	Detailed Contents	Hrs
00.	**Course Introduction** This laboratory offers hands-on experience in core cybersecurity practices through a continuous real-world simulation. Students act as analysts for a fictional organization, **TechSecure Solutions Pvt. Ltd.**, applying network security, cryptography, ethical hacking, system hardening, and digital forensics techniques to identify vulnerabilities, defend systems, and investigate incidents—gaining practical skills to secure digital environments against real-world threats..	--
01.	**Network Security and Traffic Analysis** ***Learning Objective/s:*** *Apply network-scanning and traffic-analysis techniques within the TechSecure environment to discover assets, open ports, and potential exposure points.* **Content:** Overview of cybersecurity and network threats, OSI and TCP/IP model fundamentals, IP addressing, routing, and packet structures, Network scanning and enumeration techniques, Common network attacks (DoS, MITM, ARP spoofing), Intrusion Detection and Prevention concepts, Network monitoring and traffic analysis methods **Demonstration:** **Scenario Context:** TechSecure Solutions Pvt. Ltd. has deployed a new internal network. As the cybersecurity analyst, your first task is to map the infrastructure, identify reachable hosts, and understand the normal flow of traffic to build a baseline for later monitoring. **Task 1: Network Scanning and Mapping using Nmap** — Identify live hosts, open ports, and services on a target network. **Task 2: Traffic Capture and Analysis using Wireshark** — Capture and analyze packets to identify suspicious or malicious activity.	**9-11**
	Self-Learning Topics: *Advanced intrusion detection using **Suricata**,Network log correlation and alerting systems,Wi-Fi network reconnaissance and defenses, Network segmentation and VLAN-based security*	
	Learning Outcomes: *The learner will be able to* *LO 1.1: Analyze Nmap scan results to identify live hosts, open ports, and running services within a target network. (P.I-1.4.1,2.4.2,4.3.1,11.1.2)* *LO 1.2: Analyze captured network traffic to detect and interpret suspicious or malicious activities based on packet data.(P.I-1.3.1,2.4.4,4.3.4,11.2.1)*	
02.	**Cryptography and Data Protection** ***Learning Objective:*** *Implement and assess cryptographic techniques to safeguard TechSecure's confidential data and validate its integrity.* **Content:** Fundamentals of cryptography and its role in cybersecurity, Symmetric and asymmetric encryption techniques (AES, RSA), Hashing and message authentication codes (MD5, SHA), Digital signatures and certificates,	**9-11**

	Public Key Infrastructure (PKI) overview, Steganography and covert communication techniques, Cryptanalysis and password cracking basics **Demonstration:** **Scenario Context:** During internal communication, TechSecure's HR team transmits sensitive employee records. You must secure these exchanges and ensure that data cannot be intercepted or altered. **Task 3:** Data Encryption and Decryption using OpenSSL — Implement AES and RSA encryption to protect file contents. **Task 4:** Data Hiding using Steghide — Embed secret messages in images or audio files and retrieve them securely.	
	Self-Learning Topics: Public Key Infrastructure (PKI) implementation, Elliptic Curve Cryptography (ECC) concepts, Blockchain and distributed ledger encryption, Cryptanalysis and brute-force testing tools	
	Learning Outcomes: *The learner will be able to* *LO 2.1: Analyze the effectiveness of AES and RSA encryption techniques in securing data by comparing encrypted and decrypted file contents. (P.I-1.4.1,2.1.3,5.2.2,7.1.1).* *LO 2.2: Analyze steganographic embedding and extraction processes to evaluate the integrity and confidentiality of hidden data within media files.(P.I-1.3.1,2.4.3,5.3.2,7.2.2)*	
03.	**Ethical Hacking and Vulnerability Assessment** ***Learning Objective:*** *Conduct a structured vulnerability assessment and interpret findings to recommend improvements to TechSecure's infrastructure security.* **Contents:** Ethical hacking concepts and legal considerations, Phases of penetration testing (Reconnaissance to Reporting), Vulnerability assessment and exploitation fundamentals, Common attack vectors (web, network, and wireless), Overview of OWASP Top 10 vulnerabilities, Reporting and documenting security findings, Remediation and patch management **Demonstration:** **Scenario Context:** After securing data transmissions, TechSecure requests a controlled vulnerability assessment to evaluate its new web portal and servers. **Task 5:** Vulnerability Scanning using OpenVAS — Conduct a vulnerability scan to identify and assess security weaknesses. **Task 6:** Web Application Testing using OWASP ZAP — Analyze a web application for common OWASP vulnerabilities (SQL Injection, XSS, CSRF).	**09-11**
	Self-Learning Topics: *Social engineering techniques, Exploit development fundamentals, Wireless and IoT hacking basics, Capture the Flag (CTF) competitions and practice labs*	
	Learning Outcomes: *A learner will be able to* *LO 3.1: Analyze vulnerability scan reports to identify, categorize, and assess the severity of security weaknesses in target systems. (P.I-1.4.1,2.1.2,4.1.1,5.1.1,11.1.1)* *LO 3.2: Analyze web application test results to detect and interpret common OWASP vulnerabilities such as SQL Injection, XSS, and CSRF.(P.I-1.3.1,2.4.2,4.2.1,5.2.2,11.1.2)*	

04.	**System and Endpoint Security** ***Learning Objective:*** *Evaluate system audit outputs and implement hardening controls to strengthen TechSecure's endpoint resilience.* **Contents:** Security threats to operating systems and endpoints, System hardening strategies for Windows and Linux, Patch management and configuration control, Antivirus, EDR, and firewall concepts, Malware types, lifecycle, and analysis basics, Host-based intrusion detection systems (HIDS), Backup and recovery planning **Demonstration:** **Scenario Context:** OpenVAS reports revealed several weaknesses on TechSecure's Linux systems. You will now harden these endpoints and examine potential malware that may have slipped through prior defenses. **Task 7:** System Hardening using Lynis — Conduct a security audit and apply hardening recommendations on a Linux system. **Task 8:** Malware Analysis using Cuckoo Sandbox — Execute and observe malware behavior in a controlled environment. ***Self-Learning Topics:*** *Endpoint Detection and Response (EDR) systems, Kernel-level security in Linux, automating security audits using scripts, Patch management best practices* ***Learning Outcomes:*** *A Learner will be able to* *LO 4.1: Evaluate system audit findings to determine security gaps and implement appropriate hardening measures on a Linux system. (P.I-1.4.1,2.1.1,4.1.2,5.2.1,7.1.1)* *LO 4.2:Examine malware execution reports to interpret behavioral patterns and assess potential system impacts.(P.I-1.3.1,2.4.4,4.3.1,5.2.2,7.2.2)*	
05	**Incident Response and Digital Forensics** ***Learning Objectives:*** *Perform forensic analysis of compromised systems to reconstruct the incident and identify root causes.* **Contents:** Cyber incident response lifecycle (Preparation, Detection, Containment, Eradication, Recovery), Evidence collection and chain of custody principles, File system and log analysis, Disk imaging and data preservation, Memory and volatile data acquisition, Forensic reporting and documentation standards, Introduction to threat hunting **Demonstration:** **Scenario Context:** Despite hardening, TechSecure experiences a simulated breach. You must investigate how the attacker entered, what data was accessed, and gather digital evidence. **Task 9:** Disk Forensics using Autopsy — Recover deleted files and examine metadata from a forensic disk image. **Task 10:.**Memory Forensics using Volatility — Analyze memory dumps to identify malicious processes and artifacts.	

	Self-Learning Topics: *Memory forensics in live systems, Timeline analysis and log correlation, Cloud forensics basics, Legal and ethical considerations in cyber investigations* ***Learning Outcomes:*** *A learner will be able to* *LO 5.1: Examine recovered files and metadata from a forensic disk image to determine evidence of user activity or data tampering .(P.I-1.4.1,2.4.2,4.3.1,5.1.1,11.3.1)* *LO 5.2: Evaluate memory dump artifacts to identify indicators of malicious processes and assess their impact on system integrity.(P.I-1.3.1,2.4.4,4.3.4.5.2.2,11.3.2)*	
06.	**Security Operations and Risk Management** ***Learning Objective:*** *Create and configure monitoring and risk-assessment mechanisms to maintain TechSecure's ongoing cybersecurity posture.* **Contents:** Security Operations Center (SOC) structure and functions, SIEM principles and log correlation, Threat intelligence gathering and analysis, Risk management frameworks (ISO 27001, NIST, FAIR), Business continuity and disaster recovery planning, Policy formulation and compliance auditing, Introduction to automation in security monitoring **Demonstration:** **Scenario Context:** Following the breach investigation, TechSecure establishes a small Security Operations Center (SOC) to monitor systems and quantify organizational risks for executive reporting. **Task 11:** SIEM Setup using Wazuh — Configure a basic SIEM to monitor and analyze security logs. **Task 12:** Risk Assessment using OpenFAIR — Identify and quantify organizational cybersecurity risks and propose mitigation strategies.	
	Self-Learning Topics*: Threat intelligence platforms and indicators of compromise (IOC), Automation in SOC operations using Python/Shell scripts, ISO 27001 and NIST Cybersecurity Framework overview, Business continuity and disaster recovery planning* ***Learning Outcomes:*** *A learner will be able to* *LO 6.1: Create and configure a functional SIEM setup to collect, correlate, and visualize security log data for effective threat monitoring. (P.I-1.4.1,2.4.2,3.2.2,5.2.2.6.1.1)* *LO 6.2: Develop a comprehensive risk assessment model to quantify cybersecurity risks and design suitable mitigation strategies.(P.I-1.3.1,3.1.1,2.4.4,5.3.1,6.2.1)*	
	Total	**60**

Course Outcomes:

Learner will be able to

1. Analyse network traffic and apply security measures to detect and mitigate basic network threats using open source tools.*(LO 1.1,LO 1.2)*
2. Apply encryption, hashing, and steganography techniques using open-source tools to secure sensitive data and verify its integrity.*(LO 2.1, LO 2.2)*
3. Perform vulnerability assessments using open-source tools and evaluate system weaknesses to recommend appropriate security controls.*(LO 3.1, LO 3.2)*
4. Analyse and strengthen system configurations using open-source tools to enhance endpoint security and resilience against malware.*(LO 4.1,4.2)*

5. Conduct digital forensic analysis and interpret evidence from compromised systems using open-source tools.(*LO 5.1 ,LO 5.2)*
6. Design and implement basic security monitoring and risk mitigation frameworks using open-source SIEM and assessment tools.*(LO 6.1,LO 6.2)*

CO-PO Mapping Table with Correlation Level

CO ID	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
HMLCS701.1	3	3	-	3	-	-	-	-	-	-	3
HMLCS701.2	3	3	-	-	3	-	3	-	-	-	-
HMLCS701.3	3	3	-	3	3	-	-	-	-	-	3
HMLCS701.4	3	3	-	3	3	-	3	-	-	-	-
HMLCS701.5	3	3	-	3	3	-	-	-	-	-	3
HMLCS70.16	3	3	3		3	3	-	-	-	-	-
Average	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**-**	**-**	**-**	**3**

Performance Indicators:

P.I. No.	P.I. Statement
1.3.1	Apply engineering fundamentals
1.4.1	Apply theory and principles of computer science engineering to solve an engineering problem
2.1.1	Evaluate problem statements and identifies objectives
2.1.2	Identifies processes/modules/algorithms of a computer based system and parameters to solve a problem
2.1.3	Identifies mathematical algorithmic knowledge that applies to a given problem
2.4.2	Analyze and interpret the results using contemporary tools.
2.4.3	Identify the limitations of the solution and sources/causes.
2.4.4	Arrive at conclusions with respect to the objectives.
3.1.1	Able to define a precise problem statement with objectives and scope.
3.2.2	Ability to produce a variety of potential design solutions suited to meet functional requirements.
4.1.1	Define a problem for purposes of investigation, its scope and importance
4.1.2	Ability to choose appropriate procedure/algorithm, data set and test cases.
4.2.1	Design and develop appropriate procedures/methodologies based on the study objectives
4.3.1	Use appropriate procedures, tools and techniques to collect and analyze data

4.3.4	Synthesize information and knowledge about the problem from the raw data to reach appropriate conclusions
5.1.1	Identify modern engineering tools, techniques and resources for engineering activities
5.2.1	Identify the strengths and limitations of tools for (i) acquiring information, (ii) modeling and simulating, (iii) monitoring system performance, and (iv) creating engineering designs.
5.2.2	Demonstrate proficiency in using discipline specific tools
5.3.1	Discuss limitations and validate tools, techniques and resources
5.3.2	Verify the credibility of results from tool use with reference to the accuracy and limitations, and the assumptions inherent in their use.
7.1.1	Identify situations of unethical professional conduct and propose ethical alternatives
7.2.2	Examine and apply moral & ethical principles to known case studies
11.1.1	Describe the rationale for requirement for continuing professional development
11.1.2	Identify deficiencies or gaps in knowledge and demonstrate an ability to source information to close this gap
11.2.1	Identify historic points of technological advance in engineering that required practitioners to seek education in order to stay current
11.3.1	Source and comprehend technical literature and other credible sources of information
11.3.2	Analyze sourced technical and popular information for feasibility, viability, sustainability, etc.

Text Books:

1. William Stallings, *Network Security Essentials: Applications and Standards*, Pearson Education, 6th Edition, 2023.
2. Behrouz A. Forouzan**,** *Cryptography and Network Security*, McGraw Hill, 2019.
3. Charles P. Pfleeger, Shari Lawrence Pfleeger & Jonathan Margulies**,** *Security in Computing*, Pearson, 5th Edition, 2015.
4. Matt Bishop**,** *Computer Security: Art and Science*, Addison-Wesley, 2nd Edition, 2018.
5. Dieter Gollmann**,** *Computer Security*, Wiley, 4th Edition, 2021.

Reference Books:

1. **Georgia Weidman**, *Penetration Testing: A Hands-On Introduction to Hacking*, No Starch Press, 2019
2. **Jon Erickson**, *Hacking: The Art of Exploitation*, No Starch Press, 2nd Edition, 2008.
3. **Niels Ferguson, Bruce Schneier & Tadayoshi Kohno**, *Cryptography Engineering: Design Principles and Practical Applications*, Wiley, 2010.
4. **Jason Luttgens, Matthew Pepe & Kevin Mandia**, *Incident Response and Computer Forensics*, McGraw Hill, 3rd Edition, 2014.
5. **Richard Bejtlich**, *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*, No Starch Press, 2014.
6. **Chris Sanders & Jason Smith**, *Applied Network Security Monitoring: Collection, Detection, and Analysis*, Syngress, 2013.
7. **P.W. Singer & Allan Friedman**, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, 2014.

Other Resources:

1. **NPTEL Course – "Introduction to Information Security"** By Prof. Sandeep K. Shukla | IIT Kanpur Practical Cyber Security for Cyber Security Practitioners - Course
2. **Tryhackme-** Virtual labs

A. IN-SEMESTER ASSESSMENT (50 MARKS)

1. **Mini-Project (20 Marks)**
   Design and Implementation of a Secure Network Environment with Threat Detection and Incident Response
   Project Description:
   Students shall design and implement a cybersecurity solution for a fictional organization of their choice (e.g., a healthcare provider, financial firm, educational institution, or tech startup) by creating a realistic scenario that reflects the organization's digital infrastructure and potential security challenges.

   - Using open-source tools and virtualized environments (such as VirtualBox, Docker, or VMware with Linux-based systems), students will:
   - Define the organization's structure, IT assets, and potential threat landscape.
   - Design and configure a secure network environment hosting essential services (e.g., web, file, or database servers).
   - Implement cryptographic measures to protect data in transit and at rest.
   - Perform vulnerability assessments and recommend mitigation strategies.
   - Configure open-source SIEM or IDS tools for monitoring and threat detection.
   - Simulate or analyze incidents (using controlled data or logs) and perform forensic analysis to identify root causes.
   - Document findings, mitigations, and recommendations in a comprehensive security and incident response report.
2. **Regularity and active Participation (05 Marks)**
3. **Practical Execution (15 Marks)**

Practical Setup and Tool Usage(Correct installation, configuration, and execution of open-source tools; ability to apply them effectively to the given task.)	4
Understanding of Concepts(Viva)	3
Accuracy of Execution and Results(output/results are valid, verified, and relevant to the stated objective)	4
Documentation and Reporting(Maintains clear record of procedure, screenshots, observations, and interpretation of results in the lab report)	2
Analysis and Interpretation / Presentation(Ability to analyze results, identify issues, and present findings logically)	2

4. **Case Study (10 Marks)**

A proper case study analysis on the self-learning topic or participation in the Capture the Flag competitions.

Course Type	Course Code	Course Name	Credits
HMC	HMCCS804	APPLICATION SECURITY	04

Examination Scheme					
Distribution of Marks			Exam Duration (Hrs.)		Total Marks
In-semester Assessment		End Semester Examination (ESE)			
Continuous Assessment	Mid-Semester Exam (MSE)		MSE	ESE	
20	30	50	1.5	2	100

Pre-requisite:

1. HMCCS602: Infrastructure Management

Program Outcomes addressed:

1. PO1: Engineering knowledge
2. PO2: Problem analysis
3. PO3: Design/development of solutions
4. PO 4: Conduct investigations of complex problems
5. PO5: Engineering Tool Usage
6. PO6: The Engineer and the World
7. PO 8: Individual and team work
8. PO 9: Communication
9. PO11: Life-Long Learning

Course Objectives: Learner is expected	
1.	To impart the knowledge about concepts of application Security, Threats, and Attacks.
2.	To impart knowledge of various countermeasures for the threats with respect to Application security.
3.	To introduce leaners with the need of Secure Coding Practices and the concepts of Secure Application Design and Architecture.
4.	To acquaint learner with different Security Scanning and testing techniques.
5.	To make them Analyse different threat modelling approaches.

Module	Details	Hrs.
00.	**Course Introduction** Application Security is a specialized course designed to provide learners with a deep understanding of the principles, techniques, and practices required to design and secure modern applications. It emphasizes the identification of vulnerabilities, secure coding standards, cryptographic principles, and system hardening techniques essential for protecting software from evolving cyber threats.	**01**
01.	**Introduction to Application Security, Threats, and Attacks**	**06-07**

	Learning Objective/s: *Learner is expected to map web applications through reconnaissance, discover subdomains using open-source tools, and analyse APIs to identify exposed or vulnerable endpoints.*	
	Contents: Introduction to Web Application Reconnaissance, Finding Subdomains, API Analysis, Identifying Weak Points in Application Architecture Offense: Broken Access Control, Security Misconfiguration, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), XML External Entity (XXE) Injection, Injection Attacks, Denial of Service (DoS), Cross-Origin Resource Sharing Vulnerabilities Hands-on using open-source tools(Burp Suite/ OWASP Juice shop /DVWA) for API Analysis and Endpoint Identification	
	Self-Learning Topics: *Simulate the attacks using open-source tools in virtual environment*	
	Learning Outcomes: *A learner will be able to* *LO 1.1 Apply web application reconnaissance techniques to identify potential security risks in application architecture. (P.I.-1.3.1)* *LO 1.2: Apply secure solutions for architectural weaknesses by applying systematic threat analysis and evaluating mitigation options for common web vulnerabilities. (P.I.-1.4.1)* *LO 1.3: Identify offensive web attacks to determine root causes and exploitation paths. (P.I.-2.2.2)* *LO 1.4 Identify the security posture of web applications by analysing API endpoints and identifying weak points using structured problem-analysis techniques. (P.I.-2.3.2)* *LO 1.5: Demonstrate open-source tools to perform hands-on API analysis, enumerate endpoints, and interpret testing results effectively. (P.I.- 3.2.2,5.1.1)* *LO 1.6: Develop security testing methodologies in practical scenarios and demonstrate the ability to document findings, communicate risks, and propose improvements. (P.I.-3.1.3,5.2.2)*	
02.	**Defence and Tools**	**09-11**
	Learning Objective: *Learner is expected to appraise secure architecture principles and coding practices to design, build, and defend modern web applications against a wide range of vulnerabilities and attacks*	
	Contents: Securing Modern Web Applications, Secure Application Architecture, Reviewing Code for Security, Vulnerability Discovery, Defending Against Broken Access Control, Defending against Security Misconfiguration, Defending Against XSS Attacks, Defending Against CSRF Attacks, Defending Against XXE, Defending Against Injection attacks, Defending Against DoS, defending against CORS based attacks Hands-on using open-source tools to identify, exploit, and mitigate common web application vulnerabilities	
	Self-Learning Topics: *Exploring the OWASP Top 10 and Mapping Each Risk to Real-World Web Application Security Controls.*	
	Learning Outcomes:	

	A learner will be able to *LO 2.1 Apply core engineering fundamentals and security principles to analyse modern we application architectures and identify potential vulnerabilities. (PI: 1.3.1)* *LO 2.2 Apply secure coding concepts to evaluate defence mechanisms against attacks. (PI: 1.4.* *LO 2.3 Identify core processes, modules, and parameters to analyse web application to in orde to formulate potential security threat vectors. (PI: 2.1.2)* *LO 2.4 Compare alternative mitigation techniques for identified vulnerabilities, to select the most effective method. (PI: 2.2.4)* *LO 2.5: Generate appropriate design solutions for system requirements and identify modern engineering tools needed to support their development and implementation. (PI: 3.2.2,5.1.1)* *LO 2.6 Integrate secure code modules into a web application to remediate identified vulnerabilities by demonstrating proficiency in using discipline-specific security tools. (PI: 3.4.2, 5.2.2)*	
03.	**Secure Coding Practices**	**09-11**
	Learning Objective: *Learner is expected to justify the need for defense-in-depth security strategy by implementing critical controls for data handling, authentication, and configuration to design and build web applications*	
	Contents: Security Requirements, Encryption, Never Trust System Input, Encoding and Escaping, Third-Party Components, Security Headers: Seatbelts for Web Apps, Securing Your Cookies, Passwords, Storage, and Other Important Decisions, HTTPS Everywhere, Framework Security Features, File Uploads, Errors and Logging, Input Validation and Sanitization, Authorization and Authentication, Parameterized Queries, Least Privilege, Requirements Checklist Hands On for Manual Code Verification and Validation	
	Self-Learning Topics: OWASP Secure Coding Practices	
	Learning Outcomes: *A learner will be able to* *LO 3.1 Apply engineering fundamentals and core computer science principles to evaluate input handling, and assess secure architecture decisions. (LO 1.3.1)* *LO 3.2 Apply mathematical and security engineering concepts to examine code for vulnerabilities, verify the effectiveness of controls. (LO 1.4.1)* *LO 3.3 Evaluate insecure inputs, weak authentication flows, misconfigured third-party components, improper logging, and unsafe storage practices to identify security vulnerabilities. (PI: 2.1.1)* *LO 3.4: Identify risks associated with poor error handling, missing security headers, insecure cookies, and untrusted user input using structured security review approaches. (P.I.-2.2.2)* *LO 3.5: Develop, implement, and evaluate security controls by applying suitable security tools effectively, reviewing secure code, collaborating within a group, communicating analysis results by presentation.(PIs:3.2.2, 3.4.2, 5.1.1, 5.2.2 , 8.1.1,8.2.1, 9.1.1,9.1.3, 11.1.1, 11.1.2)*	
04.	**Secure Application Design and Architecture**	**09-11**
	Learning Objectives:	

	Learner is expected to integrate security principles, defined team roles, and essential activities into every phase of the Software Development Lifecycle to proactively identify and mitigate design flaws and security bugs	
	Contents: Secure Software Development Lifecycle Averting Disaster Before It Starts, Team Roles for Security, Security in the Software Development Lifecycle, Design Flaw vs. Security Bug, Secure Design Concepts, Segregation of Production Data, Application Security Activities	
	Self-Learning Topics: *Secure Hardware architecture*	
	Learning Outcomes:	
	A learner will be able to *LO 4.1: Apply the principles of secure software development and identify design flaws versus security bugs. (PI 1.3.1)* *LO 4.2: Apply secure design concepts and the importance of segregating production data in applications. (PI 1.4.1)* *LO4.3: Identify potential security weaknesses, design flaws, and early-stage risks before implementation to analyze software designs and architectures. (PI 2.3.2)* *LO 4.4: Identify data handling, error-prone design decisions, and the absence of security controls to determine their impact on application security. (PI 2.4.3)* *LO 4.5: Analyze real-world security incidents to differentiate between design flaws to identify impacts in the life-cycle and implementation bugs. (PI 4.3.1)* *LO 4.6: Analyze security practices essential for maintaining secure software development in real-world security incidents. (PI 4.3.4)*	
05.	**Security Scanning and Testing** ***Learning Objective/s:*** *Learner is expected to identify security vulnerabilities and performance bottlenecks across the full application stack b. applying a diverse set of testing strategies and open-source tools .*	**09-11**
	Contents:	
	Testing Your Code, Testing Your Application, Testing Your Infrastructure, Testing Your Database, Testing Your APIs and Web Services, Testing Your Integrations, Testing Your Network, Dynamic Web Application Profiling Hands-on labs applying open-source tools for full-stack testing, from static code analysis and API validation to infrastructure scanning and dynamic performance profiling	
	Self-Learning Topics: Open-source Application Security Tools, IAST, RASP and WAF, Selenium	
	Learning Outcomes :	
	A learner will be able to *LO 5.1 Apply full-stack test results, identify failure patterns, interpret vulnerabilities, and draw valid conclusions on the security and reliability of application components. (PI 2.4.4)* *LO 5.2 Analyse application components and conduct systematic testing to identify vulnerabilities in code, APIs, and databases identify modern automated tools for testing web applications, APIs, and databases to detect and analyse vulnerabilities. (PI 4.3.1, PI 5.1.1))*	

	LO 5.3: Analyse infrastructure, network, and integrations through dynamic profiling to assess system security posture. (PI 2.2.2) *LO 5.4: Demonstrate proficiency in using profiling and monitoring open source tools to continuously validate web application security. (PI, 4.3.4, 5.1.1)*	
06.	**Threat Modeling** ***Learning Objective:*** *The learner is expected demonstrate threat modeling methodologies to formulate risk mitigation strategies that integrate security across the SDLC.* **Contents:** Objectives and Benefits of Threat Modeling, defining a Risk Mitigation Strategy, Improving Application Security, Building Security in the Software Development Life Cycle, Existing Threat Modeling Approaches Security, Software, Risk-Based Variants, Threat Modeling Within the SDLC ,Building Security in SDLC with Threat Modeling, Integrating Threat Modeling Within the Different Types of SDLCs ***Self-Learning Topics:*** *The Common Vulnerability Scoring System (CVSS)* ***Learning Outcomes:*** *A learner will be able to* *LO 6.1: Apply threat modelling techniques to identify potential security risks in software systems. (PI: 1.3.1)* *LO 6.2: Apply risk mitigation strategies by integrating threat modeling within various stages of the software development lifecycle. (PI: 1.4.1)* *LO 6.3: Develop tailored threat modelling workflows for two different SDLC approaches, specifying entry/exit criteria, artifacts, and team responsibilities for each phase. (PI 3.2.2)* *LO 6.4: Compare existing threat modelling approaches and select its relevance to software security improvement. (PI 2.2.4).* *LO 6.5: Design, analyse, and evaluate security risks in software systems by systematically identifying, prioritizing, and documenting threats using structured threat-modelling frameworks, and develop an effective risk mitigation strategy while communicating the analysis results clearly through group reports and presentations. (PIs: 2.2.2, 3.1.1, 8.2.1, 8.3.1, 9.1.1, 9.1.3)*	**06-07**
	Course Conclusion	**01**
	Total	**60**

Performance Indicators:

P.I. No.	P.I. Statement
1.3.1	Apply engineering fundamentals
1.4.1	Apply theory and principles of computer science engineering to solve an engineering problem
2.1.1	Evaluate problem statements and identifies objectives
2.1.2	Identifies processes/modules/algorithms of a computer based system and parameters to solve a problem
2.2.2	Identifies functionalities and computing resources.
2.2.4	Compare and contrast alternative solution/methods to select the best methods
2.3.2	identify design constraints for required performance criteria.
2.4.3	Identify the limitations of the solution and sources/causes.
2.4.4	Arrive at conclusions with respect to the objectives.
3.1.1	Able to define a precise problem statement with objectives and scope
3.1.3	Ability to review state of the art literature to synthesize system requirements.
3.1.6	Ability to develop software requirement specifications (SRS).
3.2.2	Ability to produce a variety of potential design solutions suited to meet functional requirements.
3. 3.1	Ability to perform systematic evaluation of the degree to which several design concepts meet the criteria.
3.4.2	Ability to implement and integrate the modules.
4.3.1	Use appropriate procedures, tools and techniques to collect and analyze data
4.3.4	Synthesize information and knowledge about the problem from the raw data to reach appropriate conclusions
5.1.1	Identify modern engineering tools, techniques and resources for engineering activities
5.2.2	Demonstrate proficiency in using discipline specific tool
6.3.1	Identify risks/impacts in the life-cycle of an engineering product or activity
6.3.2	Understand the relationship between the technical, socio economic and environmental dimensions of sustainability
8.2.1	Demonstrate effective communication, problem solving, conflict resolution and leadership skills
8.3.1	Present results as a team, with smooth integration of contributions from all individual efforts
9.1.1	Read, understand and interpret technical and nontechnical information
9.1.3	Create flow in a document or presentation - a logical progression of ideas so that the main point is clear
11.1.1	Describe the rationale for requirement for continuing professional development
11.1.2	Identify deficiencies or gaps in knowledge and demonstrate an ability to source information to close this gap

Course Outcomes: A learner will be able to -

1. Apply the fundamentals of security to Enumerate the terms of application Security, Threats, and

Attacks (LO 1.1, LO 1.2, LO 1.3, LO 1.4,LO1.5 ,LO1.6)

2. Illustrate the countermeasures for the threats with respect to Application security. (LO 2.1, LO 2.2, LO 2.3, LO 2.4,LO2.5 ,LO2.6)
3. Apply concepts of Application Security to Explain the Secure Application Design and Architecture and Discuss the Secure Coding Practices. (LO 3.1, LO 3.2, LO 3.3, LO 3.4, LO3.5 , LO 4.1, LO 4.2, LO 4.3, LO 4.4,LO 4.5 ,LO 4.6,)
4. Review the different Security Scanning and testing techniques. (LO 5.1, LO 5.2, LO 5.3, LO 5.4)
5. Identify the various threat modeling approaches to be used for various applications. (LO 6.1, LO 6.2, LO 6.3, LO 6.4,LO 6.5)

CO-PO Mapping Table with Correlation Level

CO ID	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
HMCCS804.1	3	3	3	-	3	-	-	-	-	-	-
HMCCS804.2	-	3	3	-	3	-	-	-	-	-	-
HMCCS804.3	-	3	3	3	3	3	-	-	-	-	3
HMCCS804.4	-	-	-	3	3	-	-	3	3	-	-
HMCCS804.5	-	-	3	3	-	-	-	3	3	-	-
Average	**3**	**3**	**3**	**3**	**3**	**3**	**-**	**3**	**3**	**-**	**-**

Text Books :

1.	Alice and Bob Learn Application Security, by Tanya Janca Wiley; 1st edition (4 December 2020).
2.	Web Application Security, A Beginner's Guide by Bryan Sullivan McGraw-Hill Education; 1st edition (16 January 2012)
3.	Web Application Security: Exploitation and Countermeasures for Modern Web Applications by Andrew Hoffman Shroff/O'Reilly; First edition (11 March 2020).
4.	The Security Development Lifecycle by Michael Howard Microsoft Press US; 1st edition (31 May 2006)

Reference Books :

1.	Software Security: Building Security In by Gary McGraw Addison-Wesley Professional; 1st edition (January 23, 2006)
2.	A Guide to Securing Modern Web Applications by Michal Zalewski
3.	Threat Modeling: A Practical Guide for Development Teams by Izar Tarandach and Matthew J. Coles Dec 8, 2020

Other Resources :

1.	Web link- https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v2.pdf https://app.cybrary.it/browse/course/advanced-penetration-testing

A. IN-SEMESTER ASSESSMENT (50 MARKS)

1. Continuous Assessment - Theory-(20 Marks)

Suggested breakup of distribution

a) Assignment on live problems/ case studies: 10 Marks

Students should be assigned a real life problem statement related to IT infrastructure management domain. Students are expected to research and collect required data to

design a system for the selected problem. Students should apply infrastructure management knowledge to design a system for IT resources including memory, network, server and storage requirements. Students should present their work in the form of presentation and demonstration in 10-15 minutes. This assignment should be graded for 10 marks like a design assignment based on the parameters such as data acquisition, requirement analysis, designing a system for selected problem statement.

b) Open notes test: 05 Marks

c) Regularity and active participation :05 Marks

d) Mid Semester Exam (30 Marks)

Mid semester examination will be based on 40% to 50% syllabus.

B. END SEMESTER EXAMINATION (50 MARKS)

End Semester Examination will be based on syllabus coverage up to the Mid Semester Examination (MSE) carrying 20%-30% weightage, and the syllabus covered from MSE to ESE carrying 70%-80% weightage.

, Course Type	Course Code	Course Name	Credits
HMC	HMCDS501	FOUNDATION OF DATA SCIENCE	03

Examination Scheme					
Distribution of Marks			Exam Duration (Hrs.)		Total Marks
In-semester Assessment		End Semester Examination (ESE)			
Continuous Assessment	Mid-Semester Exam (MSE)		MSE	ESE	
20	30	50	1.5	2	100

Pre-requisite:

NIL

Program Outcomes addressed:

1. PO1: Engineering knowledge
2. PO2: Problem analysis
3. PO3: Design/development of solutions
4. PO4: Conduct investigations of complex problems
5. PO8: Individual and Collaborative team work
6. PO9: Communication

Course Objectives:

1. To introduce Fundamental Data Science Concepts
2. To familiarize Students with Data Classification and Statistical Analysis
3. To impart Knowledge of Data Analysis and Visualization Tools
4. To introduce Exploratory Data Analysis and Machine Learning Preparation
5. To impart Teamwork Skills and Familiarize Students with Modern Data Science Tools

Module	Details	Hrs.
00.	**Course Introduction** This is a sample paragraph, Overview of course, application of course in Industry/real life problem. This is foundation course which deals with fundamental concepts of force flow and its effect on mechanical components. The fundamental concepts of this subject are essential for designing the mechanical components on strength criteria.	01
01.	**INTRODUCTION** ***Learning Objective:*** ***To impart the knowledge of the tools, techniques, and processes involved in data science, laying the groundwork for more advanced topics in the field.***	02-04

	Contents: Data Science: Benefits and uses , facets of data, Data Science Process: Overview , Defining research goals , Retrieving data, Data preparation,Exploratory Data analysis , build the model,presenting findings and building applications, Data Mining , Data Warehousing , Basic Statistical descriptions of Data	
	Self-Learning Topics: ***How to clean and prepare your data will significantly improve the performance and accuracy of any subsequent machine learning models you build, and ensure that your analysis is based on high-quality, structured data.***	
	Learning Outcomes: *A learner will be able to* *LO 1.1: Use mathematical and statistical techniques, such as probability and numerical methods, to analyze and interpret data in data science applications. (PI- 1.1.1)* *LO 1.2: Use computer science and engineering principles to retrieve, process, and analyze large datasets, applying data science techniques to real-world challenges. (PI- 1.4.1)* *LO 1.3: identify the required computing resources, tools, and technologies for efficient data retrieval, preparation, and model building in data science projects. (PI-2.2.2)* *LO 1.4: Use modern data analysis tools to explore, visualize, and interpret data, ensuring accurate insights and informed decision-making. (PI-2.4.2)*	
02.	**DESCRIBING DATA**	**07-09**
	Learning Objective: ***To make learner to identify and classify different types of data and variables, Summarize data effectively using tables and visualizations., Calculate and interpret averages and measures of variability to understand data distribution. and Recognize the significance of normal distributions and z-scores in statistical analysis and apply these concepts to real-world data.***	
	Contents: Types of Data, Types of Variables, Describing Data with Tables and Graphs, Describing Data with Averages , Describing Variability, Normal Distributions and Standard (z) Scores	
	Self-Learning Topics: ***Describing Data with Averages and Variability: Understanding Central Tendency and Spread***	
	Learning Outcomes: *A learner will be able to* *LO 2.1: Use computer science and engineering concepts to classify different types of data and variables. Organize and display data using tables and graphs. Set clear goals when analyzing data with averages and variability. Use visual tools to explain statistical results, including normal distributions and standard (z) scores. (PI-1.4.1)* *LO 2.2: Recognize different types of data and variables and represent them effectively using tables and graphs. Calculate averages and measure variability to summarize and describe data distributions. (PI-2-1.1)* *LO 2.3: Use basic engineering and math skills to classify different types of data and variables. Organize and present data using tables and graphs. Perform*	

	statistical calculations, such as averages and variability, to analyze data distributions. Read and interpret technical information to understand normal distributions and standard (z) scores. (PI- 1.3.1) *LO 2.4: Analyze normal distributions and standard (z) scores to interpret statistical results. Assess findings, draw meaningful conclusions, and ensure alignment with data analysis objectives (PI-2-4.4)*	
03.	**DESCRIBING RELATIONSHIPS** ***Learning Objective:*** *To impart the knowledge of Calculating and interpret correlation coefficients to assess the strength and direction of relationships. Use regression analysis to fit a line to data, make predictions, and understand the nature of the relationship between variables.*	**10-12**
	Contents: Correlation ,Scatter plots ,correlation coefficient for quantitative data ,computational formula for correlation coefficient ,Regression ,regression line ,least squares regression line ,Standard error of estimate ,interpretation of r2 ,multiple regression equations ,regression towards the mean	
	Self-Learning Topics: ***Understanding Correlation and Regression: Exploring Relationships Between Variables***	
	Learning Outcomes: *A learner will be able to* *LO 3.1: Analyze relationships between variables using correlation and regression techniques. Create scatter plots and compute correlation coefficients to identify data patterns. Explore and compare different approaches for analyzing data relationships. (PI- 3.2.1)* *LO 3.2: Apply regression methods, including the least squares line and multiple regression, to make predictions. Interpret r2r^2r2 to evaluate model accuracy and explain regression toward the mean. Use engineering principles to enhance data analysis and modeling techniques. (PI- 1.4.1)* *LO 3.3: Explore relationships between variables using correlation and regression techniques. Create scatter plots and compute correlation coefficients to measure data connections. Evaluate different approaches to data analysis and select the most effective method for problem-solving. (PI- 3.2.2)* *LO 3.4: Apply regression methods, including the least squares line and multiple regression, to make predictions. Interpret the standard error, r2r^2r2, and regression toward the mean using mathematical and engineering principles to improve data analysis accuracy. (PI- 1.3.1)*	
04.	**PYTHON LIBRARIES FOR DATA WRANGLING** ***Learning Objectives:*** ***To make learner understand Efficiently manipulate numerical and structured data using NumPy arrays. Apply aggregation, filtering, and mathematical operations to NumPy arrays for advanced data analysis. Master key features of Pandas such as data indexing, selection, cleaning, and handling missing data and Combine and merge multiple datasets efficiently for more comprehensive analysis.***	**06-08**
	Contents: Basics of Numpy arrays ,aggregations,computations on arrays ,comparisons, masks, boolean logic, fancy indexing ,structured arrays, Data manipulation with Pandas ,data indexing and selection , operating on data ,missing data , Hierarchical indexing , combining datasets , aggregation and grouping , pivot tables	

	Self-Learning Topics: ***Data Manipulation with Pandas: Indexing, Selection, and Handling Missing Data***	
	Learning Outcomes: *A learner will be able to* *LO 4.1: Apply Engineering Fundamentals for Data Manipulation Using NumPy and Pandas (PI- 1.3.1)* *LO 4.2: Apply Computer Science Principles for Data Processing Using NumPy and Pandas (PI-1.4.1)* *LO 4.3: Apply NumPy to create and manage arrays, perform calculations, and use advanced indexing techniques like masking and fancy indexing. Use Pandas to organize, filter, and clean data, handle missing values, and combine datasets for effective data analysis..(PI- 2.2.2)* *LO 4.4: Use Pandas to group datasets, create pivot tables, and extract meaningful insights. Apply modern data analysis tools to interpret technical information and support informed decision-making. ..(PI- 5.1.1)* *LO 4.5: Utilize NumPy to create and manage arrays, perform calculations, and apply techniques like masking, boolean logic, and fancy indexing. Use Pandas to organize, filter, and clean data, handle missing values, and merge datasets for effective analysis. (PI-2.4.2)* *LO 4.6: Generate pivot tables, analyze data using modern tools, and present findings through clear visualizations. Apply advanced data processing techniques to extract insights and support informed decision-making in team-based projects..(PI-5.1.2)*	
05.	**DATA VISUALIZATION** ***Learning Objective/s:*** ***To familiarize learner various types of plots, including line, scatter, density, histograms, and contour plots, to represent data effectively. Visualize error and uncertainty in your data using error bars and understand how to highlight key data points through annotations and legends. Create customized visualizations, including color schemes, subplots, and 3D plots, to suit different data contexts and Work with geographic data using Basemap for mapping locations and spatial patterns..***	**07-09**
	Contents: Importing Matplotlib, Line plots,Scatter plots ,visualizing errors , density and contour plots , Histograms , legends ,colors ,subplots ,text and annotation ,customization , three dimensional plotting ,Geographic Data with Basemap ,Visualization with Seaborn.	
	Self-Learning Topics: ***Data Visualization with Matplotlib and Seaborn: Creating Informative and Customizable Plots***	
	Learning Outcomes :	
	A learner will be able to *LO 5.1: Apply Computer Science Principles for Data Visualization Using Matplotlib and Seaborn (P-: 1.4.1)* *LO 5.2: Apply Engineering Fundamentals for Data Visualization Using Matplotlib and Seaborn (PI-1.3.1)* *LO 5.3: Import and use Matplotlib and Seaborn to generate various visualizations, including line plots, scatter plots, histograms, density plots, and 3D plots. Enhance*	

	visualizations by adding legends, colors, subplots, text, and annotations to effectively analyze and present data. (PI- 2.4.2) *LO 5.4: Apply Basemap for geographic data visualization and use Seaborn to identify patterns in datasets. Explore and compare different visualization techniques to present insights clearly and effectively in team-based projects(PI-3.2.1)* *LO 5.5 : Generate various charts using Matplotlib and Seaborn, including line plots, scatter plots, histograms, and 3D plots. Apply modern tools to create visualizations, interpret technical information, and present data clearly.. (PI-2.2.2)* *LO 5.6 Enhance visualizations by incorporating colors, labels, legends, and text for improved clarity. Explore and compare different visualization techniques to select the most effective method for clear and accurate data representation. (PI-3.2.2)*	
06.	**EXPLORATORY DATA ANALYSIS** ***Learning Objective/s:*** ***To make Learner to develop a strong foundation in*** *data cleaning, preparation, exploration, and analysis****, providing the skills necessary to effectively apply machine learning algorithms in real-world scenarios***	**05-07**
	Contents: Need of exploratory data analysis, cleaning and preparing data, Feature engineering, Missing values, understand dataset through various plots and graphs, draw conclusions, deciding appropriate machine learning models.	
	Self-Learning Topics: *Exploratory Data Analysis (EDA) and Data Preprocessing: Cleaning, Feature Engineering, and Visualization*	
	Learning Outcomes: *A learner will be able to* *LO 6.1: Apply Engineering Fundamentals for Exploratory Data Analysis and Machine Learning Preparation (PI- 1.3.1)* *LO 6.2: Apply Computer Science Principles for Exploratory Data Analysis and Machine Learning Preparation (PI- 1.4.1)* *LO 6.3: L Clean and prepare data by handling missing values and applying feature engineering techniques. Utilize various plots and graphs to analyze datasets, extract meaningful insights, and select appropriate machine learning models. Collaborate effectively in a team, use modern data analysis tools, interpret technical information, explore different problem-solving approaches. (PI-2.2.2, 3.2.2,5.1.1, 8.1.1, 9.1.1)* *LO 6.4: Clean and preprocess data by handling missing values and applying feature engineering techniques. Use graphs and charts to explore datasets, identify patterns, and make data-driven decisions. Select appropriate machine learning models based on insights gained from data analysis. Collaborate effectively in a team to interpret results, present findings visually, and stay updated with emerging data science techniques. (PI-2.4.2, 3.2.1, 5.1.2, 8.3.1, 9.3.1)*	
	Course Conclusion	**01**
	Total	**45**

Performance Indicators:

P.I. No.	P.I. Statement
1.1.1	Apply the knowledge of discrete structures, linear algebra, statistics and numerical techniques to solve problems
1.3.1	Apply engineering fundamentals
1.4.1	Apply theory and principles of computer science engineering to solve an engineering problem
2.2.2.	Identifies functionalities and computing resources
2.4.2.	Analyze and interpret the results using contemporary tools
3.2.1	Ability to explore design alternatives
3.2.2	Ability to produce a variety of potential design solutions suited to meet functional requirements.
4.1.2	Ability to choose appropriate procedure/algorithm, data set and test cases.
4.3.1	Use appropriate procedures, tools and techniques to collect and analyze data
5.1.1	Identify modern engineering tools, techniques and resources for engineering activities
5.1.2	Create/adapt/modify/extend tools and techniques to solve engineering problems
8.1.1	Recognize a variety of working and learning preferences; appreciate the value of diversity on a team
8.3.1	Present results as a team, with smooth integration of contributions from all individual efforts
9.1.1	Read, understand and interpret technical and nontechnical information
9.3.1	Create engineering-standard figures, reports and drawings to complement writing and presentations

Course Outcomes: A learner will be able to -

1. Use probability, numerical methods, and statistical techniques such as regression and correlation to analyze and interpret data. *(LO 1.1, 1.2, 1.3, 1.4)*
2. Classify classify and represent data using tables and graphs, compute relationships using correlation and regression, and analyze normal distributions and variability. *(LO 2.1, 2.2, 2.3, 2.4, 3.1, 3.2, 3.3, 3.4)*
3. Demonstrate proficiency in using NumPy and Pandas for data manipulation and Matplotlib and Seaborn for creating various types of data visualizations. *(LO 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6)*
4. Clean clean and preprocess datasets, handle missing values, apply feature engineering, and use statistical methods to select appropriate machine learning models. *(LO 6.1, 6.2, 6.3, 6.4)*
5. Work collaboratively on data science projects, apply modern computing tools for data analysis, and continuously update their knowledge to keep up with evolving trends. *(LO 6.3, 6.4)*

CO-PO Mapping Table with Correlation Level

CO ID	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
HMCDS501.1	3	3	-	-	-	-	-	-	-	-	-
HMCDS501.2	3	3	3	-	-	-	-	-	-	-	-
HMCDS501.3	3	3	3	-	3	-	-	-	-	-	-
HMCDS501.4	3	3	3	-	3	-	-	3	3	-	-
HMCDS501.5	-	3	3	-	3	-	-	3	3	-	-
Average	**3**	**3**	**3**	-	**3**	-	-	**3**	**3**	-	-

.

Text Books :

1. David Cielen, Arno D. B. Meysman, and Mohamed Ali, "Introducing Data Science", Manning Publications, 2016. (Unit I)
2. Robert S. Witte and John S. Witte, "Statistics", Eleventh Edition, Wiley Publications, 2017. (Units II and III)
3. Jake VanderPlas, "Python Data Science Handbook", O'Reilly, 2016. (Units IV and V)

Reference Books :

1. Allen B. Downey, "Think Stats: Exploratory Data Analysis in Python", Green Tea Press,2014.

Other Resources :

1. NPTEL Course: Data Science for EngineersBy Prof. Ragunathan Rengasamy, Prof. Shankar Narasimhan | IIT Madras
:-Web link- https://nptel.ac.in/courses/108/101/108101037/

A. IN-SEMESTER ASSESSMENT (50 MARKS)

1. Continuous Assessment - Theory-(20 Marks)

Suggested breakup of distribution

a) Development of Working model for demonstration of concept:10M

· A group of 3 students should be assigned a real life problem statement.

· Students are expected to research and collect required resources to create a frontend and backend for the selected problem.

· Students should prepare a presentation of 10-15 minutes.

b) Article reading & summarization activity: : 05 Marks

c) Regularity & Active participation: 05 Marks

1. Mid Semester Exam (30 Marks)

Mid semester examination will be based on 40% to 50% syllabus.

B. END SEMESTER EXAMINATION (50 MARKS)

End Semester Examination will be based on syllabus coverage up to the Mid Semester Examination (MSE) carrying 20%-30% weightage, and the syllabus covered from MSE to ESE carrying 70%-80% weightage.

Course Type	Course Code	Course Name	Credits
HMC	HMCDS602	DATA SCIENCE FOR HEALTHCARE	03

Examination Scheme					
Distribution of Marks			Exam Duration (Hrs.)		Total Marks
In-semester Assessment		End Semester Examination (ESE)			
Continuous Assessment	Mid-Semester Exam (MSE)		MSE	ESE	
20	30	50	1.5	2	100

Pre-requisite:

1. HMCDS501 Foundation of Data Science

Program Outcomes addressed:

1. PO1: Engineering knowledge
2. PO2: Problem analysis
3. PO3: Design/development of solutions
4. PO4: Conduct investigations of complex problems
5. PO5: Engineering Tool Usage
6. PO7: Ethics
7. PO11: Life-Long Learning

Course Objectives:

1. To introduce the perspective of Data Science for Health Care.
2. To make learner apply different techniques of Biomedical Image Analysis.
3. To impart the knowledge of NLP techniques for processing Clinical text.
4. To introduce the role of social media analytics for Healthcare data
5. To make learner learn advanced analytics techniques for Healthcare Data and investigate the current scope, potential, limitations, and implications of data science and its applications for healthcare.

Module	Details	Hrs.
00.	**Course Introduction** Data science and healthcare course focus on application of data science in healthcare domain. The healthcare industry produces massive amounts of valuable data on patient demographics, treatment plans, medical examination results, insurance, etc. Data science and big data analytics can provide practical insights and assist in the decision-making process for strategic healthcare decisions. It contributes to developing a comprehensive picture of patients, customers, and	**01**

	clinicians. Data-driven decision-making opens up new avenues for improving healthcare.	
01.	**Introduction to Data Science and Healthcare** ***Learning Objective:*** *To make learner identify and summarize the data sources of Healthcare domain and understand benefits of Electronic Health Record.*	**05-07**
	Contents: Introduction, Healthcare Data Sources and Data Analytics for Healthcare, Applications and Practical Systems for Healthcare. Electronic Health Records(EHR), Components of EHR, Benefits of EHR, Barriers to Adopting EHR, Challenges of using EHR data, Phenotyping Algorithms	
	Self-Learning Topics: *Identify electronic Health Record Case study.* ***Learning Outcomes:*** *A learner will be able to* *LO1.1: Apply concepts of data science to healthcare system (P.I.-1.1.1)* *LO1.2: Apply concepts to find the challenges of using electronic health record (P.I.-1.3.1)* *LO1.3: Identify different data sources for healthcare (P.I.-2.1.2)* *LO1.4: Identify components electronic health record and its benefits (P.I.-2.2.2)*	
02.	**Biomedical Image Analysis** ***Learning Objective:*** *To familiarize with the different Biomedical Imaging models, comprehend and apply different image preprocessing techniques on healthcare data.*	**08-10**
	Contents: Biomedical Imaging Modalities, Object detection, Image segmentation, Image Registration, Feature Extraction. Mining of Sensor data in Healthcare, Challenges in Healthcare Data Analysis, Biomedical Signal Analysis, Genomic Data Analysis for Personalized Medicine **Demonstration of Image preprocessing techniques using open source tool**	
	Self-Learning Topics: *Image preprocessing on identified case study under consideration.* ***Learning Outcomes:*** *A learner will be able to* *LO2.1: Identify different Biomedical Imaging models. (P.I.-2.1.2)* *LO2.2: Compare different Biomedical Imaging models to select best model (P.I.-2.2.4)* *LO2.3: Apply different image preprocessing techniques on healthcare data. (P.I.-1.3.1)* *LO2.4: Apply different data analysis techniques on healthcare data. (P.I.-1.4.1)*	

03.	**Data Science and Natural Language Processing for Clinical Text** ***Learning Objective:*** *To impart the knowledge of analysis of different approaches to mining information from clinical text and challenges in processing clinical reports*	**06-08**
	Contents: NLP, mining information from Clinical Text, Information Extraction, Rule Based Approaches, Pattern based algorithms, Machine Learning Algorithms. Clinical Text Corpora and evaluation metrics, challenges in processing clinical reports, Clinical Applications. **Demonstration of Information Extraction techniques using open source tool**	
	Self-Learning Topics: *Information extraction from case study under consideration.* ***Learning Outcomes:*** *A learner will be able to* *LO3.1: Apply different approaches to mining information from clinical text. (P.I.-1.3.1)* *LO3.2: Apply different NLP approaches to mining information from clinical text (P.I.-1.4.1)* *LO3.3: Identify different challenges in processing clinical reports. (P.I.-2.2.3)* *LO3.4: Identify methodology to Solve challenges in processing clinical reports. (P.I.-2.1.2)*	
04.	**Social Media Analytics for Healthcare** ***Learning Objective:*** *To familiarize with social media analysis of infectious disease outbreak and apply Algorithms for social media analysis for public Health Research.*	**06-08**
	Contents: Basics of Social Media Analytics, Social Media analysis for detection and tracking of Infectious Disease outbreaks. Outbreak detection, Social Media Analysis for Public Health Research, Analysis of Social Media Use in Healthcare. **Demonstration of Social Media analysis techniques using open source tool**	
	Self-Learning Topics: *Social media analysis of case study under consideration* ***Learning Outcomes:*** *A learner will be able to* *LO4.1: Synthesize information of social media for infectious disease outbreak. (P.I.- 4.3.4)* *LO4.2: Identify appropriate techniques/ algorithms for social media analysis. (P.I.- 4.1.2, 5.1.1)* *LO4.3: Identify use of Social Media use in Healthcare (P.I.- 2.2.3)* *LO4.4: Identify techniques/ Algorithms used to solve social media analysis problems for public Health Research (P.I.-2.1.3, 5.1.2)*	
05.	**Advanced Data Analytics for Healthcare**	**06-08**

	Learning Objective: *To make learner aware of the different clinical prediction models and temporal data mining techniques for healthcare data.*	
	Contents: Review of Clinical Prediction Models, Temporal Data Mining for Healthcare Data, Visual Analytics for Healthcare Data, Information Retrieval for Healthcare- Data Publishing Methods in Healthcare. **Demonstration of data publishing methods of Information Retrieval using open source tool**	
	Self-Learning Topics: *Clinical Prediction model for case study under consideration.* ***Learning Outcomes:*** *A learner will be able to* *LO5.1: Identify and apply Clinical Prediction Models for healthcare data using modern engineering tools. (P.I.-1.4.1, 5.1.1)* *LO5.2: Apply Temporal Data Mining for Healthcare Data. (P.I.-1.3.1)* *LO5.3: Identify and analyze the results of application of Visual Analytics techniques using modern tools for Healthcare data to solve engineering problems (P.I.-2.4.2, 5.1.2)* *LO5.4: Identify Information Retrieval-Data Publishing Methods in Healthcare. (P.I.-2.2.3)*	
06.	**Data Science Practical Systems for Healthcare** ***Learning Objective:*** *To make learner aware of Data Analytics for different Healthcare system like, Fraud Detection in Healthcare, Pharmaceutical discoveries and biomedical data, etc.*	**06-08**
	Contents: Data Analytics for Pervasive Health, Fraud Detection in Healthcare. Data Analytics for Pharmaceutical discoveries, Clinical Decision Support Systems. Computer-Assisted Medical Image Analysis Systems- Mobile Imaging and Analytics for Biomedical Data. **Demonstration of Fraud Detection techniques in Healthcare using open source tool**	
	Self-Learning Topics: *Future Data science Trends in the Healthcare Industry* ***Learning Outcomes:*** *A learner will be able to* *LO6.1: Design Healthcare system like, Fraud Detection in Healthcare, Pharmaceutical discoveries and biomedical data with ethical alternatives. (P.I.- 3.2.1, 7.1.1)* *LO6.2: Design Clinical Decision Support Systems based on moral & ethical principles. (P.I.- 3.4.2, 7.2.2)* *LO6.3: Identify and Select data for pervasive health analysis (P.I.- 2.1.2, 11.2.1)* *LO6.4: Analyze data using Computer-Assisted Medical Image feasibility Analysis Systems for sustainability (P.I.- 2.2.3, 11.3.2)*	
	Course Conclusion	**01**

Total	**45**

Performance Indicators:

P.I. No.	P.I. Statement
1.1.1	Apply the knowledge of discrete structures, linear algebra, statistics and numerical techniques to solve problems
1.3.1	Apply engineering fundamentals
1.4.1	Apply theory and principles of computer science engineering to solve an engineering problem
2.1.2	Identifies processes/modules/algorithms of a computer based system and parameters to solve a problem
2.1.3	Identifies mathematical algorithmic knowledge that applies to a given problem
2.2.2	Identifies functionalities and computing resources.
2.2.3	Identify existing solution/methods to solve the problem, including forming justified approximations and assumptions
2.2.4	Compare and contrast alternative solution/methods to select the best methods
2.4.2	Analyze and interpret the results using contemporary tools
3.2.1	Ability to explore design alternatives
3.4.2	Ability to implement and integrate the modules
4.1.2	Ability to choose appropriate procedure/algorithm, data set and test cases.
4.3.4	Synthesize information and knowledge about the problem from the raw data to reach appropriate conclusions
5.1.1	Identify modern engineering tools, techniques and resources for engineering activities
5.1.2	Create/adapt/modify/extend tools and techniques to solve engineering problems
7.1.1	Identify situations of unethical professional conduct and propose ethical alternatives
7.2.2	Examine and apply moral & ethical principles to known case studies
11.2.1	Identify historic points of technological advance in engineering that required practitioners to seek education in order to stay current
11.3.2	Analyse sourced technical and popular information for feasibility, viability, sustainability, etc.

Course Outcomes: A learner will be able to -

1. Identify and apply appropriate Data Science technique for Health Care. *(LO1.1, LO1.2, LO1.3, LO1.4*)
2. Analyse and Apply different techniques of Biomedical Image Analysis. *(LO2.1, LO2.2, LO2.3*, *LO2.4)*
3. Apply NLP techniques for processing Clinical text data. *(LO3.1, LO3.2, LO3.3, LO3.4)*
4. Analyse role of social media analytics for Healthcare data using engineering tools. *(LO4.1, LO4.2, LO4.3, LO4.4)*
5. Design applications for healthcare using advanced analytics techniques and tools with ethical consideration. *(LO5.1, LO5.2, LO5.3, LO5.4, LO6.1, LO6.2, LO6.3, LO6.4)*

CO-PO Mapping Table with Correlation Level

CO ID	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
HMCDS602.1	3	3	-	-	-	-	-	-	-	-	-
HMCDS602.2	3	3	-	-	-	-	-	-	-	-	-
HMCDS602.3	3	3	-	-	-	-	-	-	-	-	-
HMCDS602.4	-	3	-	-	3	-	-	-	-	-	-

HMCDS602.5	3	3	3		3	-	-	-	-	-	-
Average	**3**	**3**	**3**	**3**	**3**	-	-	-	-	-	-

Text Books :

1. Chandan K. Reddy and Charu C Aggarwal, "Healthcare data analytics", Taylor & Francis, 2015.
2. Hui Yang and Eva K. Lee, "Healthcare Analytics: From Data to Knowledge to Healthcare Improvement, Wiley, 2016
3. Madsen, L. B. (2015). Data-driven healthcare: how analytics and BI are transforming the industry. Wiley India Private Limited
4. Strome, T. L., & Liefer, A. (2013). Healthcare analytics for quality and performance improvement. Hoboken, NJ, USA: Wiley

Reference Books :

1. McNeill, D., & Davenport, T. H. (2013). Analytics in Healthcare and the Life Sciences: Strategies, Implementation Methods, and Best Practices. Pearson Education
2. Arvin Agah, "Medical applications of Artificial Systems ", CRC Press
3. Sergio Consoli Diego Reforgiato Recupero Milan Petković,"Data Science for Healthcare-Methodologies and Applications", Springer
4. Dac-Nhuong Le, Chung Van Le, Jolanda G. Tromp, Gia Nhu Nguyen, "Emerging technologies for health and medicine", Wiley.
5. Ton J. Cleophas • Aeilko H. Zwinderman, "Machine Learning in Medicine- Complete Overview", Springer
6. Arjun Panesar, "Machine Learning and AI for Healthcare", A Press.

Other Resources :

1. NPTEL Course: NOC: Exploring Survey Data on Health Care, By Prof. Pratap C. Mohanty Department of Humanities and Social Sciences, IIT Roorkee.
   Web link- https://nptel.ac.in/courses/109107190
2. NPTEL Course: Health Research Fundamentals, Department of Humanities and Social Sciences, National Institute of Epidemiology.
   Web link- https://onlinecourses.nptel.ac.in/noc21_hs62/preview

A. IN-SEMESTER ASSESSMENT (50 MARKS)

1. Continuous Assessment - Theory-(20 Marks)

Suggested breakup of distribution

a) One Assignment on live problems/ case studies: 10 Marks

Students should be assigned a real life problem statement related to healthcare domain. Students are expected to research and collect required data to design a system for the selected problem. Students should apply data science techniques for preprocessing, model building, testing, and validation. Students should present their work in the form of presentation and demonstration in 10-15 minutes. This assignment should be graded for 10 marks like a mini project based on the parameters such as data acquisition, requirement analysis, design, model building and testing for selected problem statement.

b) One Think Pair Share (TPS) activity: 05 Marks

c) Regularity and active participation: 05 Marks

2. Mid Semester Exam (30 Marks)

Mid semester examination will be based on 40% to 50% syllabus.

B. END SEMESTER EXAMINATION (50 MARKS)

End Semester Examination will be based on syllabus coverage up to the Mid Semester Examination (MSE) carrying 20%-30% weightage, and the syllabus covered from MSE to ESE carrying 70%-80% weightage.

Course Type	Course Code	Course Name	Credits
HMC	HMCDS703	SOCIAL MEDIA ANALYTICS	04

Examination Scheme					
Distribution of Marks			Exam Duration (Hrs.)		Total Marks
In-semester Assessment		End Semester Exam (ESE)			
Continuous Assessment	Mid-Semester Exam (MSE)		MSE	ESE	
20	30	50	1.5	2	100

Pre-requisite:

1. Artificial intelligence and Data Science I and II
2. Data Mining and BI

Program Outcomes addressed:

1. PO1: Engineering knowledge
2. PO2: Problem analysis
3. PO3: Design/Development of Solutions
4. PO4: Conduct Investigations of Complex Problems
5. PO5: Engineering Tool Usage
6. PO6: Engineer and world
7. PO11: Life-long learning

Course Objectives:

1. To know the fundamental concepts, components, and importance of social media analytics in supporting data-driven decision-making across various domains.
2. To develop knowledge of social media data collection methods, preprocessing steps, and analytical techniques for handling large, unstructured data.
3. To apply sentiment analysis, text mining, and social network analysis methods to extract meaningful insights from social media platforms.
4. To enable learners to visualize, interpret, and report social media trends using effective analytical and visualization tools.
5. To equip students with the ability to implement social media analytics techniques in real-world case studies and practical applications.

Module	Detailed Contents	Hrs
00.	**Course Introduction** Social Media Analytics (SMA) is an interdisciplinary field that focuses on collecting, measuring, analyzing, and interpreting data from social media platforms to generate meaningful insights. With billions of users actively generating content every day, social media has become a powerful source of information for understanding human behavior, brand perception, public opinion, and real-time events.	01
01.	**Introduction to Social Media Analytics** ***Learning Objective:*** *Learner is expected to recall and interpret data structures and algorithms to solve real time-complex issues and maximize results. Collect and manage social media data using APIs, scraping tools, and platform insights dashboards.* **Contents:** Overview of social media and its types (Facebook, Twitter/X, Instagram, LinkedIn, YouTube, Reddit, etc.), Nature and characteristics of social media data. Importance of analytics in social media, Applications: marketing, politics, business intelligence, crisis management, Ethical, privacy, and legal considerations in social media analysis ***Self-Learning Topics:*** *Various Social Media Platforms and data availability* ***Learning Outcomes:*** *A learner will be able to* *LO 1.1: Apply the concepts of computing theory in modelling of computer-based system functionalities and data analytics. (P.I. 1.1.2)* *LO 1.2: Apply theory and principles of computer science engineering to solve social media analytics and associated problems. (P.I. 1.4.1)* *LO 1.3: Identifies functionalities and characteristics of social media. (P.I.-2.2.2)* *LO 1.4: Identify various social media platforms and the types of data they generate (text, image, video, metadata, interaction data). (P.I.-2.2.3)* *LO 1.5: Identify the characteristics, structure, and nature of data across major platforms such as Twitter, Facebook, Instagram, YouTube, Reddit, LinkedIn, and TikTok. (P.I.-2.4.3)* *LO 1.6: Able to identify and document system requirements on comparison of different social media data sources based on accessibility, data format, volume, user behaviour, and analytical suitability. (P.I. 3.1.4)* *LO 1.7: Able to explore design alternatives for defined problem in social media analytics w.r.t. various types of data collections. (P.I. 3.2.1)*	07-09
02.	**Social Media Data Collection** ***Learning Objective:*** *Learners should able to apply data preprocessing techniques to clean, filter, and prepare unstructured text and multimedia data for analysis.*	09-11
	Contents: APIs for data access (Twitter API, Facebook Graph API, YouTube API, etc.) , Web scraping fundamentals (BeautifulSoup, Selenium), Data storage: JSON,	

	MongoDB, CSV, Streaming data and real-time collection, Handling rate limits and authentication	
	Self-Learning Topics: *Study different platforms (X/Twitter, Instagram, YouTube, LinkedIn, Reddit) structure content, engagement, reach, and algorithms.*	
	Learning Outcomes: *A learner will be able to* *LO 2.1: Apply the concepts of computing theory for social media data collection and analytics. (P.I. 1.1.2)* *LO 2.2: Apply appropriate data collection techniques for platforms like Twitter (X), Facebook, Instagram, YouTube, Reddit, and LinkedIn. (P.I.- 1.4.1)* *LO 2.3: Identifies functionalities and characteristics various APIs for data access. (P.I.-2.2.2)* *LO 2.4: Identify various methods and tools used for collecting social media data (APIs, web scraping, third-party tools, streaming services). (P.I.-2.2.3)* *LO 2.5: Able to identify and document collected data sheet in required format for processing. (P.I.-3.1.2)* *LO 2.6: Explore and synthesize system requirements from larger social and professional concerns. (P.I. 3.1.5)* *LO 2.7: Identify modern engineering tools, techniques and resources for social media analytics. (P.I. 5.1.1)* *LO 2.8: Modify tools and techniques to solve engineering problems in social media data. (P.I. 5.1.2)*	
03.	**Data Preprocessing and Text Mining** ***Learning Objective:*** *Convert textual data into meaningful representations using methods such as Bag-of-Words, TF–IDF, n-grams, and basic word embeddings.*	**10-12**
	Contents: Cleaning and preprocessing social media data, Tokenization, stop-word removal, stemming, lemmatization, Hashtag and mention analysis. Feature extraction: TF-IDF, word embeddings, Topic modelling (LDA)	
	Self-Learning Topics: *Study platform-specific metrics like impressions, reach, views, CTR, and engagement rate.*	
	Learning Outcomes: *A learner will be able to* *LO 3.1: Apply the knowledge of linear algebra, statistics and numerical techniques to solve computational problems. (P.I. 1.1.1)* *LO 3.1: Apply techniques for handling missing data, inconsistent formats, duplicates, and irrelevant information in text datasets. (P.I.-1.4.1)* *LO 3.2 Identifies functionalities and characteristics text mining tools. (P.I.-2.2.2)* *LO 3.3: Identify the importance of preprocessing techniques for improving the quality and usability of raw textual data. (P.I.-2.2.3)* *LO 3.4: Able to identify and document collected data sheet to formulate the data mining model. (P.I.-3.1.2)*	

	LO 3.5: Ability to perform essential text preprocessing steps such as tokenization, stop-word removal, stemming, lemmatization, normalization, and noise filtering. (P.I.-3.3.1) *LO 3.6: Identify modern engineering tools, techniques and resources for social media analytics for data pre-processing and text mining. (P.I. 5.1.1)* *LO 3.7: Modify tools and techniques to solve engineering problems in social media data. (P.I. 5.1.2)*	
04.	**Sentiment and Opinion Mining** ***Learning Objective:*** *Conduct sentiment and opinion mining to classify and interpret user attitudes, emotions, and perceptions.*	**03-05**
	Contents: Sentiment analysis approaches (lexicon-based and machine learning-based), Tools and libraries: NLTK, Text Blob, VADER, transformers Emotion detection and polarity scoring, Case studies: brand monitoring, election prediction, product reviews	
	Self-Learning Topics: *Try free or trial versions of tools like Hootsuite, Brandwatch, Talkwalker, Google Trends.*	
	Learning Outcomes: *A learner will be able to* *LO 4.1: Apply text preprocessing and feature extraction techniques specifically tailored for sentiment and opinion mining tasks. (P.I.-1.4.1)* *LO 4.2: Identifies various sentiment and opinion mining techniques. (P.I.-2.2.2)* *LO 4.3: Identify appropriate approach of implementations of rule-based, lexicon-based, and machine learning-based approaches for sentiment classification. (P.I.-2.2.3)* *LO 4.4: Able to identify and document collected data for sentiment mining model. (P.I.-3.1.2)* *LO 4.5: Explore and synthesize system requirements from larger social and professional concerns on sentiment analysis techniques to classify text into categories such as positive, negative, neutral, or emotion-specific labels. (P.I.-3.1.5)* *LO 4.6: Design and develop appropriate procedures/methodologies to analyze user-generated content from social media, reviews, blogs, and forums to extract sentiments and contextual opinions (P.I 4.2.1)* *LO 4.7: Define the purpose of investigation and identify modern engineering tools, techniques and resources for social media analytics for sentiment analysis and opinion mining. (P.I. 4.1.1, P.I. 5.1.1)* *LO 4.8: Identify the strengths and limitations of tools for acquiring information, monitoring system performance of SMA models. (P. I. 5.2.1)* *LO 4.9: Identify and describe various engineering roles to interpret sentiment insights to support decision-making in areas like marketing, customer analytics, and social media monitoring. (P.I. 1.3.1, P. I. 6.1.1)*	
05.	**Social Network Analysis** *Learning Objective: Learner should able to use network analysis techniques to support real-world applications such as recommendation systems, marketing strategies, and crisis detection.*	**05-07**

	Contents: Basics of graph theory for social networks, Centrality measures: degree, betweenness, closeness, Community detection and clustering, Influence and diffusion in social networks, Tools: Gephi, NetworkX	
	Self-Learning Topics: *Try using NetworkX or Gephi to visualize small social networks.*	
	Learning Outcomes: *A learner will be able to* *LO 5.1: Apply community detection algorithms like modularity-based clustering, Louvain, and Girvan–Newman. (P.I.-1.4.1)* *LO 5.2 Identifies various social network analysis tools and techniques. (P.I.-2.2.2)* *LO 5.3: Identify influential users, information diffusion patterns, and group behaviour in social media networks. (P.I.-2.2.3)* *LO 5.4: Able to identify and document collected data over social media networks. (P.I.-3.1.2)* *LO 5.5: Ability to perform graph operations and compute network statistics using Python or other analytics tools. (P.I.-3.3.1)* *LO 5.6: Define a problem for purposes of investigation, its scope and importance. (P.I. 4.1.1)* *LO 5.7: Design and develop appropriate procedures/methodologies based on the study network connectivity, clustering, and small-world phenomena. (P.I.-4.2.1)* *LO 5.8: Identify modern engineering tools, techniques and resources to compute and interpret metrics such as degree centrality, closeness, betweenness, eigenvector centrality, and density. (P.I.-5.1.1, P.I. 11.3.1)* *LO 5.9: Create//modify/ tools and techniques to solve various real-life problem of social media, (P.I. 5.1.2)* *LO 5.10: Interpret legislation, regulations of social data privacy and uses. (P.I. 1.3.1, P.I.6.2.1)*	
06.	**Visualization and Reporting** ***Learning Objective/s:*** *Explain the principles of effective data visualization and the role of visual analytics in interpreting social media insights.*	**03-05**
	Contents: Data visualization for social media insights (matplotlib, seaborn, Power BI, Tableau), Dashboards for social analytics, Trend analysis and visual storytelling, Case study: End-to-end analysis project using Twitter data	
	Self-Learning Topics: *Read recent papers on social media analytics, misinformation detection, and influence modelling*	
	. ***Learning Outcomes:*** *A learner will be able to* *LO 6.1: Apply best practices such as avoiding misleading visuals, using appropriate scales, and ensuring accessibility. (P.I.-1.4.1)* *LO 6.2: Identify appropriate visualization techniques for different types of social media data (text, network, time series, sentiment). (P.I.-2.1.2)*	

	LO 6.3 Identifies various social media visualizations tools and techniques. (P.I.-2.2.2) *LO 6.4: Able to identify and document collected data over social media problem. (P.I.-3.1.2)* *LO 6.5: Explore and synthesize system requirements from large volume of social media forms, data, jukeboxes etc. (P.I.-3.1.5)* *LO 6.6: Ability to choose appropriate hardware/software tools such as Gephi, NetworkX, or specialized analytics platforms to visualize and analyze networks. (P.I.-4.1.3)* *LO 6.7: Define problem for purpose of investigation and identify and describe various engineering roles w.r.t. social media data and network analysis. (P.I. 4.1.1, P.I.-6.1.1)* *LO 6.8: Identify modern engineering tools, techniques and resources to compute and interpret metrics such as degree centrality, closeness, betweenness, eigenvector centrality, and density. (P.I.-5.1.1)* *LO 6.9: Create//modify/ tools and techniques to solve various real-life problem of social media, (P.I. 5.1.2)* *LO 6.10: Analyze sourced technical and popular social media information for feasibility, viability and sustainability. (P.I. 1.3.1, P.I. 11.3.2)*	
	Course Conclusion	**01**
	Total	**60**

Performance Indicators:

P.I. No.	**P.I. Statement**
1.4.1	Apply theory and principles of computer science engineering to solve an engineering problem.
2.1.2	Identifies processes/modules/algorithms of a computer-based system and parameters to solve a problem
2.2.3	Identify existing solution/methods to solve the problem, including forming justified approximations and assumptions.
2.4.3	Identify the limitations of the solution and sources/causes.
3.1.2	Able to identify and document system requirements from stake holders.
3.1.4	Ability to choose appropriate quality attributes as defined by ISO/IEC/IEEE standard.
3.1.5	Explore and synthesize system requirements from larger social and professional concerns.
3.3.1	Ability to perform systematic evaluation of the degree to which several design concepts meet the criteria.
4.1.2	Ability to choose appropriate procedure/algorithm, data set and test cases.
4.1.3	Ability to choose appropriate hardware/software tools to conduct the experiment.
4.2.1	Design and develop appropriate procedures/methodologies based on the study objectives
5.1.1	Identify modern engineering tools, techniques and resources for engineering activities
5.2.1	Identify the strengths and limitations of tools for (i) acquiring information, (ii) modeling and simulating, (iii) monitoring system performance, and (iv) creating engineering designs.
5.3.1	Discuss limitations and validate tools, techniques and resources.
6.1.1	Identify and describe various engineering roles; particularly as pertains to protection of the public and public interest at global, regional and local level
6.2.1	Interpret legislation, regulations, codes, and standards relevant to your discipline and explain its contribution to the protection of the public

11.3.2 Analyze sourced technical and popular information for feasibility, viability, sustainability, etc.

Course Outcomes:

Learner will be able to

1. Apply the fundamentals and techniques of social media analytics to analyze real-world social media data and derive meaningful insights for decision-making. *(LO 1.1,LO 1.2,)*
2. Collect and preprocess social media data using APIs and Python tools. *(LO 2.1,LO 2.2, LO 2.3,LO 2.4,LO 2.5, LO 2.6, LO 3.1,LO 3.2, LO 3.3,LO 3.4, LO 3.5, LO 3.6)*
3. Perform text mining and sentiment analysis on social data. *(LO 4.1,LO 4.2, LO 4.3,LO 4.4, LO 4.5, LO 4.6, LO 4.7)*
4. Apply social network analysis techniques to identify influence and trends. (*LO 5.1, LO 5.2, LO 5.3,LO 5.4, LO 5.5, LO 5.6, LO 5.7)*
5. Visualize and interpret insights for decision-making using dashboards and reports. (*LO 6.1,LO 6.2, LO 6.3,LO 6.4, LO 6.5, LO 6.6, LO 6.7)*

CO-PO Mapping Table with Correlation Level

CO ID	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
HMCDS703.1	3	3	3	-	-		-	-	-	-	-
HMCDS703.2	3	3	3	-	3		-	-	-	-	-
HMCDS703.3	3	3	3	3	3	2	-	-	-	-	-
HMCDS703.4	3	3	3	3	3	2	-	-	-	-	2
HMCDS703.5	3	3	3	3	3	2	-	-	-	-	2
Average	**3**	**3**	**3**	**3**	**3**	**3**	-	-	-	-	2

Text Books:

1. Matthew A. Russell, *Mining the Social Web*, O'Reilly Media.
2. Marshall Sponder, *Social Media Analytics: Effective Tools for Building, Interpreting, and Using Metrics*.
3. Gohar F. Khan, *Creating Value with Social Media Analytics*.

Reference Books:

1. Q. Guo et al., *Social Media Mining and Analytics*, Springer.
2. Research papers and case studies from IEEE, ACM, and Elsevier journals.

Other Resources:

Digital material:

1. Web Link-Complete DS Data Structure in one shot | Semester Exam | Hindi (youtube.com)
2. Web Link-https://topperworld.in/dsa-handwritten-notes/

A. IN-SEMESTER ASSESSMENT (50 MARKS)

1. Continuous Assessment (20 Marks)

Suggested breakup of distribution

a) Numerical Assignment/s (Minimum 20 problems) : 05 Marks

b) Class Test based on above numerical assignment: 05 Marks

c) One Flip classroom activity: 05 Marks

d) Regularity and active participation :05 Marks

2. Mid Semester Examination (30 Marks)

Mid semester examination will be based on 40% to 50% syllabus.

B. END SEMESTER EXAMINATION (50 MARKS)

End Semester Examination will be based on syllabus coverage up to the Mid Semester Examination (MSE) carrying 20% to 30% weightage, and the syllabus covered from MSE to ESE carrying 70% to 80% weightage.

Course Type	Course Code	Course Name	Credits
HML	HMLDS701	DATA ANALYTICS LABORATORY	02

Examination Scheme					
Distribution of Marks			Exam Duration (Hrs.)		Total Marks
In-semester Assessment		End Semester Exam (ESE)			
Continuous Assessment	Mid-Semester Exam (MSE)		MSE	ESE	
50	--	--	--	--	50

Pre-requisite:

1. ITSBL301: Python Laboratory

Program Outcomes addressed :

1. PO1: Engineering knowledge
2. PO2: Problem analysis
3. PO3:Design/development of solutions
4. PO4: Conduct investigations of complex problems
5. PO5: Engineering tool usage
6. PO8: Individual and collaborative team work
7. PO9: Communication
8. PO11: Life-long learning

Course Objectives:

Learner is expected to

1. To inculcate comprehensive knowledge of data analytics using Python.
2. To learn the essential concepts of data analytics and data visualization.
3. To acquire the knowledge of supervised/unsupervised learning techniques.

Module	Detailed Contents	Hrs
00.	**Course Introduction** Data Analytics is the science of analyzing data to convert information to useful knowledge. This knowledge could help in understanding the world better, and in many contexts it enables to make better decisions. While this is broad and grand objective, the last 20 years has seen steeply decreasing costs to gather, store, and process data, creating an even stronger motivation for the use of empirical approaches to problem solving. This course seeks to present with a wide range of data analytic techniques and is structured around the broad contours of the different types of data analytics, namely, descriptive, inferential, predictive, and prescriptive analytics. Data analytics enables organizations to utilize their data to support informed decision-making, optimize operations, and explore. It gives businesses a competitive advantage by allowing them to make faster, data-driven choices, stimulate innovation, and ensure long-term growth.	--

01.	**Introduction to Data Analytics** ***Learning Objective:*** *To impart the knowledge of numpy and pandas library*	**5-10**
	Contents: • Definition, types of analytics (descriptive, diagnostic, predictive, prescriptive), applications in business, healthcare, social media, etc. **Task 1:** Group discussion on analytics applications and identify data-driven problems ***Deliverables: Problem Statement and idea presentation***	
	Learning Outcomes : *A learner will be able to* LO1.1: *Identify and analyze real-world applications of data analytics across domains with measurable variables and formulate analytical objectives (P.I. - 1.1.1, P.I. - 1.3.1, P.I. - 2.1.1, P.I. - 2.2.2, PI 9.2.2*)	
02.	**Data, Data Sources and Data Pre-processing:** *Learning Objective:* *To inculcate EDA concept and learn different visualization techniques* **Contents** **Data and Data Sources :** Types of data (structured, semi-structured, unstructured), data formats (CSV, JSON, XML), data acquisition from APIs and databases, data storage and retrieval. **Data Preprocessing** : Handling missing values, outliers, duplicates; data transformation, encoding, scaling, normalization; introduction to feature engineering. **Task 2:** Data Acquisition (APIs, Web Scraping, SQL Databases) and Data Preprocessing of the acquired data set ***Deliverables: Cleaned Dataset***	**5-10**
	Learning Outcomes: *The learner will be able to* *LO2.1: Acquire data from multiple sources (APIs, web pages, and databases) and adapt appropriate preprocessing techniques to select relevant features to enhance data quality (P.I. - 2.1.2, PI - 2.2.2, P.I. -3.3.1, P.I. - 3.4.2, P. I. 4.2.1, P. I. 4.3.1, P.I.- 5.1.1, P.I. - 5.1.2)*	
03.	**Exploratory Data Analysis (EDA) and Data Visualization:** ***Learning Objective:*** *To learn the concept of ML/DL and apply it to real world problems.* **Contents** • Descriptive statistics, correlation, distributions, identifying data patterns, feature relationships. • Principles of visualization, types of charts and plots, dashboards, data storytelling, visualization tools (Tableau / Power BI / Plotly etc.) **Task 3:** Perform EDA and apply data visualization techniques to develop dashboard for data interpretation **Deliverables:** ***EDA report and initial findings***	**18-20**

	Learning Outcomes: *The learner will be able to* *The learner will be able to* *LO3.1: Perform statistical analysis and adapt appropriate visualization techniques to represent data insights with appropriate engineering tool. (**Data Analysis**) (P.I. - 2.1.2, P.I. - 2.4.2, P.I.- 5.1.1, P.I. - 5.1.2)*	
04.	**Supervised and Unsupervised learning:** *Learning Objective:* *To learn the concept of ML/DL and apply it to real world problems.* **Contents** • Concept of supervised learning and unsupervised learning, difference between regression and classification, problem framing, feature-target relationships. • Regression Models and Classification Models **Task 4:** Apply supervised and unsupervised algorithm to develop a ML models and perform Optimization ***Deliverables: Optimized model performance report***	**08-10**
	Learning Outcomes: *The learner will be able to* *LO4.1: Identify and use appropriate algorithms to design and train the ML/DL model for set objectives, (**Methodology**). (P.I. -3.3.1, P.I. -3.4.2, P.I.-5.1.1, P.I.-5.1.2, P.I.-8.3.1, P.I. -8.2.1, P.I.-9.2.2, , P.I. -9.3.2, P.I. - 11.3.1, P.I. - 11.1.1)*	
05.	**Model Optimization** *Learning Objective:* *To learn the concept of ML/DL and apply it to real world problems.* **Contents** • Feature selection, hyperparameter tuning (GridSearchCV, RandomizedSearchCV), cross-validation (K-Fold). • Model Validation and Performance Analysis: Evaluating model accuracy and reliability using performance metrics (MAE, MSE, RMSE, Accuracy, Precision, Recall, F1-score etc.). **Task 5:** Perform model evaluation using performance metrics ***Deliverables: Model evaluation summary***	**08-10**
	Learning Outcomes: *The learner will be able to* *LO5.1: Assess model accuracy using appropriate metrics and present results with appropriate visualization in document and presentation (Results) (P.I. -2.4.1, P.I.-2.1.2, P.I.-4.3.1 P.I.- 4.2.1)*	
	Total	**60**

Performance Indicators:

P. I. Number	**P. I. Statement**
1.1.1	Apply the knowledge of discrete structures, linear algebra, statistics and numerical techniques to solve problems
1.3.1	Apply engineering fundamentals.
2.1.1	Evaluate problem statements and identifies objectives

2.1.2 Identifies processes/modules/algorithms of a computer based system and parameters to solve a problem
2.2.2 Identifies functionalities and computing resources.
2.4.1 Applies engineering mathematics to implement the solution.
2.4.2 Analyze and interpret the results using contemporary tools.
3.3.1 Ability to perform systematic evaluation of the degree to which several design concepts meet the criteria.
3.4.2 Ability to implement and integrate the modules.
4.2.1 Design and develop appropriate procedures/methodologies based on the study objectives
4.3.1 Use appropriate procedures, tools and techniques to collect and analyze data
5.1.1 Identify modern engineering tools, techniques and resources for engineering activities
5.1.2 Create/adapt/modify/extend tools and techniques to solve engineering problems
5.2.2 Demonstrate proficiency in using discipline specific tools
8.2.1 Demonstrate effective communication, problem solving, conflict resolution and leadership skills
8.3.1 Present results as a team, with smooth integration of contributions from all individual efforts
9.2.2 Deliver effective oral presentations to technical and non-technical audiences
9.3.2 Use a variety of media effectively to convey a message in a document or a presentation
11.1.1 Describe the rationale for requirement for continuing professional development
11.3.1 Source and comprehend technical literature and other credible sources of information

Course Outcomes:

Learner will be able to

1. Apply and analyze real-world applications of data analytics across domains (*LO 1.1)*
2. Apply appropriate preprocessing techniques to select relevant features to enhance data quality (*LO 2.1)*
3. Perform exploratory data analysis (EDA) using statistical and visualization techniques to derive meaningful insights (*LO 3.1*).
4. Implement and demonstrate supervised / unsupervised learning models. (*LO4.1)*.
5. Evaluate the trained models and optimize their performance. *(LO 5.1)*.
6. Design and develop full-fledged data analytics dashboard to solve the real-world problem. (*LO 1.1, LO2.1, LO 3.1, LO 4.1, LO 4.2, LO 5.1)*

CO-PO Mapping Table with Correlation Level

CO ID	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
HMLDS701.1	3	3	-	-	-	-	-	-	3	-	-
HMLDS701.2	-	3	3	3	3	-	-	-	-	-	-
HMLDS701.3	-	3	-	-	3	-	-	-	-	-	-
HMLDS701.4	-	-	3	3		-	-	-	-	-	-
HMLDS701.5	-	-	3	-	3	-	-	3	3	-	3
HMLDS701.6	-	-	3	-	3	-	-	-	-	-	-
Average	**3**	**3**	**3**	**3**	**3**	-	-	**3**	**3**	-	**3**

A. CONTINUOUS ASSESSMENT (50 MARKS)

Suggested breakup of distribution

a) Task/Project Evaluation: 20 Marks

- A group of 3 students should be assigned a real life problem statement.
- Students are expected to research and collect required resources to create a frontend and backend for the selected problem.
- Students should prepare a presentation of 10-15 minutes.
- This project should be graded for 45 marks depending on the following activity table.

Sr. No.	Task	Activity	Deliverables	Marks
1	**Task 1:** Group discussion on analytics applications and identify data-driven problems	1.Introduction to Data Analytics & Project-Based Learning 2.Formation of project teams 3.Idea presentation	***Problem Statement and idea presentation***	5
2	**Task 2:** Data Acquisition (APIs, Web Scraping, SQL Databases) and data preprocessing of the	4.Data Acquisition: APIs, Web Scraping, Databases 5.Data Cleaning & Preprocessing	***Cleaned Dataset***	3
3	**Task 3:** Perform EDA and apply data visualization techniques to develop dashboard for data interpretation	6.Exploratory Data Analysis (EDA) 7.Selection of data visualization techniques to develop dashboard for data interpretation	***EDA report and initial findings*** ***Interactive dashboard prototype***	5 5
4	**Task 4:** Apply supervised and unsupervised algorithm to develop a ML models and perform Optimization	8.Model Training (Predictive Modeling: Regression & Classification)	***Baseline ML models***	7
5	**Task 5:** Perform model evaluation using performance metrics	9. Advanced Models & hyper parameter tuning	***Optimized model performance report***	5
		10. Model Evaluation & Validation	***Model evaluation summary***	5
		11. Result Interpretation & Visualization	***Final dashboards***	5
		12. Final Project Presentation & Viva	***Project report, presentation & GitHub repo***	5
				45

c) Regularity & Active participation: 05 Marks

B. END SEMESTER EXAMINATION (Oral Exam) (25 Marks)

Suggested breakup of distribution

a) Project Presentation: 10 Marks

b) Results and discussion, Inferences drawn from the above task: 05 Marks

c) Oral based on entire syllabus: 10 Marks

Two examiners, one Internal and one External will do the evaluation

Text Books:

1. Wes McKinney, "Python for Data Analysis",O'REILLY, ISBN:978-1-449-31979-3, 1st edition, October 2012.
2. Hastie, Trevor, et al.; The elements of statistical learning. Vol. 2. No. 1. New York: Springer, 2009.
3. Montgomery, Douglas C., and George C. Runger.; Applied statistics and probability for engineers. John Wiley & Sons,2010

Reference Books:

1. Rachel Schutt & O'neil, "Doing Data Science", O'REILLY, ISBN:978-1-449-35865-5, 1st edition, October 2013.
2. Matt Harrison, "Learning the Pandas Library: Python Tools for Data Munging, Analysis, and Visualization , O'Reilly, 2016.

Other Resources:

1. NPTEL Course: Introduction to Data Analytics, IIT Madras, Prof. Nandan Sudarsanam, Prof. Balaraman Ravindran, IIT Madras, Web Link- https://nptel.ac.in/courses/110106072
2. Data Analytics Tutorial Web Link- https://www.w3schools.com/datascience/

Course Type	Course Code	Course Name	Credits
HMC	HMCDS804	MARKETING & FINANCIAL ANALYTICS	04

Examination Scheme					
Distribution of Marks			Exam Duration (Hrs.)		Total Marks
In-semester Assessment		End Semester Exam (ESE)			
Continuous Assessment	Mid-Semester Exam (MSE)		MSE	ESE	
20	30	50	--	--	100

Program Outcomes addressed :

1. PO1: Engineering knowledge
2. PO2: Problem analysis
3. PO3:Design/development of solutions
4. PO4: Conduct investigations of complex problems
5. PO5: Engineering tool usage
6. PO8: Individual and collaborative team work
7. PO9: Communication
8. PO11: Life-long learning

Course Objectives:
Learner is expected to

1. To inculcate comprehensive knowledge of data science using Python.
2. To learn the essential concepts of data analytics and data visualization.
3. To acquire the knowledge of machine learning and deep learning techniques.

Module	Detailed Contents	Hrs
00.	**Course Introduction** The Marketing & Financial Analytics course introduces students to the use of data analytics for making informed business decisions in both marketing and finance. It focuses on understanding, analyzing, and interpreting data to evaluate marketing performance, customer behavior, financial health, and profitability. Students learn to apply analytical tools such as Excel, Python, and Power BI to real-world business problems, gaining hands-on experience with data visualization, forecasting, and decision modeling.	--
01.	**Introduction to Marketing & Financial Analytics** ***Learning Objective:*** *To impart the knowledge of the fundamentals of analytics in marketing and finance and recognize their role in data-driven decision-making.*	07–09
	Contents: Definition, Scope, and Importance of Marketing & Financial Analytics. Product, Price, Place, Promotion (4P's), Financial Statements: Balance Sheet,	

	Income Statement, Cash Flow Statement, Summarize Marketing Data: Data Preparation, Slicing and Dicing, Data Summary using Graph, Making decision by summarizing the marketing data, Understanding Marketing Environment, Data driven decision making, evolution of business analytics. Types of analytics: Descriptive, Diagnostic, Predictive, Prescriptive. Tools and technologies: Excel, Power BI, Python, R, Overview of data sources: Marketing data, Financial data, CRM systems. Applications of analytics in business decision making, Exploratory Factor Analysis	
	Self-Learning Topics: *- Case studies on data-driven marketing campaigns.* *- Overview of analytics platforms used in industry.*	
	Learning Outcomes : *A learner will be able to* *LO1.1: Apply knowledge of statistics to explain the role of analytics in marketing and finance. (PI 1.1.1)* *LO1.2: Apply theory and principles of slicing, dicing and summarizing marketing data to make decisions (PI 1.4.1)* *LO1.3: Evaluate problem statements and Identify different types of analytics for business applications. (2.1.1)* *LO1.4: Apply engineering fundamentals to explore the CRM (PI 1.3.1)* *LO1.5: Identify functionalities and analyze real-world use cases for data-driven decision-making using modern engineering tool. (PI 2.2.2, PI 5.1.1,PI 5.1.2)* *LO1.6: Apply exploratory factor analysis (statistical technique) to find the underlying structure in a large set of variables. (PI 1.1.1)*	
02.	**Marketing Analytics Tools and Techniques** ***Learning Objective:*** *To inculcate knowledge of analytical tools and models to evaluate marketing performance and customer behavior.*	09–11
	Contents • Demand Forecasting: Naïve Method, Least Square Method, Regression Method, Decomposition Method, Time Series Analysis, • Marketing metrics and KPIs: CAC, CLV, ROI, churn, and conversion rates. • Segmentation, Targeting, Positioning (STP) using clustering/classification. Market Basket Analysis and Recency-Frequency- Monetary value (RFM) Modeling. • Regression and correlation analysis for sales forecasting. Digital Marketing Analytics: Google Analytics, social media metrics, Campaign analysis and visualization dashboards.	
	Self-Learning Topics: *-Use of Google Analytics and Tableau in marketing analytics.* *- Case study: Customer segmentation and campaign optimization.*	
	Learning Outcomes: *The learner will be able to* *LO2.1: Apply theory and principles of predictive and statistical analysis on marketing datasets to achieve objectives and scope. (PI 1.4.1)* *LO2.2: Evaluate problem statements, identify and compute marketing metrics for performance measurement. (PI 2.1.1)* *LO2.3: Analyze and interpret the results using Market Basket Analysis. (PI 2.4.2).*	

	LO2.4: Apply RFM modeling to implement the segment customers based on their purchase history. (PI 2.4.1) *LO2.5: Apply fundamentals of regression and correlation analysis for sales forecasting (PI 1.1.1)*	
03	**Financial Analytics and Modelling** ***Learning Objective:*** *To inculcate quantitative and computational techniques for financial analysis and decision-making.*	09–11
	Contents • Financial data analysis and time series forecasting, Ratio analysis and financial performance indicators, Forecasting revenue, profitability, and cash flows • Risk and Portfolio Analytics: VaR, Monte Carlo, optimization, Scenario and sensitivity analysis, Predictive analytics: Credit scoring, fraud detection, bankruptcy prediction.	
	Self-Learning Topics: *- Building financial dashboards using Power BI/Excel.* *- Case study: Predicting stock trends using regression models.*	
	Learning Outcomes: *The learner will be able to* *LO3.1: Analyze and interpret financial data to identify trends and patterns. (PI 2.4.2)* *LO3.2: Apply algorithm to develop financial models for forecasting and valuation. (PI 2.4.1)* *LO3.3: Apply fundamentals of risk analysis to identify financial risk in problem statement. (PI 1.3.1)* *LO3.4: Apply theory and principles of predictive analytics for fraud detection (PI 1.4.1)*	
04.	**Product and Pricing Analytics:** ***Learning Objective:*** *To learn the concept of place and promotion Analytics.*	06–09
	Contents • Product Design: Conjoint Analysis, Moving Average, Linear and Non-linear pricing, Price Optimization, Price Bundling, Discounted Pricing Price Skimming, Revenue Management, Markdown Pricing	
	Learning Outcomes: *The learner will be able to* *The learner will be able to* *LO4.1: Identify and apply moving average knowledge that helps in product selection and design (PI 2.1.3).* *LO4.2: Apply theory and principles for price prediction and analysis (PI 1.4.1).* *LO4.3: Analyze and interpret the impact of pricing strategies on customer demand and profitability by visualization method (PI 2.4.2).* *LO4.4: Apply science to perform systematic evaluation and communicate analytical insights in pricing (PI 1.2.1)*	
05.	**Place and Promotion Analytics:** ***Learning Objective:*** *To learn the concept of place and promotion Analytics.*	07–10
	Contents	

	• Designing Retail Outlet, Online Product Assortment: Market Basket Analysis • Allocating Retail Space and Sales Resources: Trade Economics, Catalog/Email Marketing. Data Visualization and Communication in Analytics: Visualization principles and storytelling with data. Designing dashboards using Power BI/Tableau. Visual analytics for decision-making. Reporting techniques. ***Self-Learning Topics:*** ***-*** *Explore visualization case studies in marketing and finance.* - Learn dashboard customization techniques. ***Learning Outcomes:*** *The learner will be able to* *LO5.1: Use market basket analysis to analyze data for optimize assortment planning (PI.4.3.1).* *LO5.2: Analyze demand patterns, cost structures, and customer behavior to identify factors influencing retail space allocation decisions. (PI 2.1.2)* *LO5.3: Analyze data patterns and user requirements to identify key variables that inform effective visualization and reporting decisions (PI 2.2.3).* *LO5.4: Prepare professional analytical reports using data and presentations to communicate findings clearly and accurately (P.I. 4.3.3, PI 5.1.1, PI 5.1.2)* *LO5.5:*	
6	**Emerging Trends and Applications in Marketing & Financial Analytics:** ***Learning Objective:*** *To explore recent developments and innovations in marketing and financial analytics.* **Contents** • AI and ML in marketing and finance. • Automation, realtime analytics, and blockchain applications. • Ethical issues and data privacy (GDPR, CCPA). • Case studies: Personalization, dynamic pricing, credit risk management ***Self-Learning Topics:*** *- Research on AI applications in marketing and finance.* *- Explore data ethics and compliance frameworks.* ***Learning Outcomes:*** *The learner will be able to* *LO6.1: Analyze how automation, real-time analytics, and blockchain technologies enhance operational efficiency and data security in business environments (PI 2.2.2).* *LO6.2: Apply analytical understanding to real-world case studies such as personalization, dynamic pricing, and credit risk management (PI 2.4.1)* *LO6.3: Identify and apply (implement) AI algorithms to real-world case studies (PI 3.4.2, P.I.-8.3.1, P.I. -8.2.1, P.I.-9.2.2, , P.I. -9.3.2, P.I. - 11.3.1, P.I. - 11.1.1).* *LO6.4: Choose appropriate algorithm, data set considering marketing and financial area. (PI 4.1.2)* *LO6.5: Validate AI/ML solutions using real-time analytical methods and performance metrics for decision-making effectiveness. (PI 4.3.1)* *LO6.6: Perform systematic evaluation of models for the marketing and financial analytics related case studies. (PI 3.3.1, P.I.-9.2.2, , P.I. -9.3.2, P.I. - 11.3.1, P.I. - 11.1.1)*	06–10
	Total	**60**

Performance Indicators:

P. I. Number	P. I. Statement
1.1.1	Apply the knowledge of discrete structures, linear algebra, statistics and numerical techniques to solve problems
1.2.1	Apply laws of natural science to an engineering problem
1.3.1	Apply engineering fundamentals.
1.4.1	Apply theory and principles of computer science engineering to solve an engineering problem
2.1.1	Evaluate problem statements and identifies objectives
2.1.2	Identifies processes/modules/algorithms of a computer based system and parameters to solve a problem
2.1.3	Identifies mathematical algorithmic knowledge that applies to a given problem
2.2.2	Identifies functionalities and computing resources.
2.2.3	Identify existing solution/methods to solve the problem, including forming justified approximations and assumptions
2.4.1	Applies engineering mathematics to implement the solution.
2.4.2	Analyze and interpret the results using contemporary tools.
3.3.1	Ability to perform systematic evaluation of the degree to which several design concepts meet the criteria.
3.4.2	Ability to implement and integrate the modules.
4.1.2	Ability to choose appropriate procedure/algorithm, data set and test cases.
4.3.1	Use appropriate procedures, tools and techniques to collect and analyze data
4.3.3	Represent data (in tabular and/or graphical forms) so as to facilitate analysis and explanation of the data, and drawing of conclusions
5.1.1	Identify modern engineering tools, techniques and resources for engineering activities
5.1.2	Create/adapt/modify/extend tools and techniques to solve engineering problems
8.2.1	Demonstrate effective communication, problem solving, conflict resolution and leadership skills
8.3.1	Present results as a team, with smooth integration of contributions from all individual efforts
9.2.2	Deliver effective oral presentations to technical and non-technical audiences
9.3.2	Use a variety of media effectively to convey a message in a document or a presentation
11.1.1	Describe the rationale for requirement for continuing professional development
11.3.1	Source and comprehend technical literature and other credible sources of information

Course Outcomes:

Learner will be able to

1. Apply statistical and analytical methods for decision-making in marketing and finance business. (*LO 1.1, LO 1.2, LO 1.3, LO 1.4,LO 1.5, LO 1.6*).
2. Utilize exploratory data analysis (EDA), marketing metrics, and statistical models for segmentation, targeting, forecasting in marketing analytics. (*LO2.1, LO2.2, LO2.3, LO2.4, LO 2.5*)
3. Analyze and evaluate financial models for forecasting, valuation, and risk analysis using advanced analytical techniques. (*LO3.1, LO3.2, LO3.3, LO3.4)*.
4. Apply theory and principles for price prediction and evaluate pricing strategies for profitability.(*LO4.1, LO4.2, LO4.3, LO4.4)*
5. Analyze and implement retail, place, and promotion analytics using visualization, dashboard design, and storytelling tools for data-driven decision-making. (*LO5.1, LO5.2, LO 5.3, LO 5.4)*
6. Evaluate and apply AI, automation in marketing and finance through case-based applications with result presentation. *(LO6.1, LO6.2, LO6.3, LO6.4, LO6.5, LO6.6)*

CO-PO Mapping Table with Correlation Level

CO ID	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
HMCDS804.1	3	3	-	-	3	-	-	-	-	-	-
HMCDS804.2	3	3	-	-	-	-	-	-	-	-	-
HMCDS804.3	3	3	-	-	-	-	-	-	-	-	-
HMCDS804.4	3	3	-	-	-	-	-	-	-	-	-
HMCDS804.5	-	3	-	3	3	-	-	-	-	-	-
HMCDS804.6	-	3	3	3	-	-	-	3	3	-	3
Average	**3**	**3**	**3**	**3**	**3**	**-**	**-**	**3**	**3**	**-**	**3**

Text Books:

1. Financial Analytics (Pitabas Mohanty) — Author: Pitabas Mohanty. Published by Wiley India. ISBN 9789354644177. 1st edition, published ~2023.
2. Marketing Analytics: Data-Driven Techniques with Microsoft Excel, Wayne L. Winston, Wiley

Reference Books:

1 Mastering Financial Analytics — Authors: Dr R Gopal, Dr Vani Kamath, Dr Priya Vij (from source) Paperback, more general overview of analytics in finance

2 Marketing Analytics, Seema Gupta, Avadhoot Jathar, Wiley

Other Resources:

1. NPTEL Course: Introduction to Marketing research and Analytics, IIT Madras, Prof. Nandan Sudarsanam, Prof. Balaraman Ravindran, IIT Madras,
   Web Link- https://nptel.ac.in/courses/110106072
2. NPTEL Course: Introduction to Data Analytics, IIT Madras, Prof. Nandan Sudarsanam, Prof. Balaraman Ravindran, IIT Madras,
   Web Link- https://nptel.ac.in/courses/110106072

A. IN-SEMESTER ASSESSMENT (50 MARKS)

1. Continuous Assessment (20 Marks)

Suggested breakup of distribution

a) One Assignment on live problems/ case studies: 10 Marks Students should be assigned a real life problem statement (different for each student). Students are expected to research and collect

required resources to solve the problem. This assignment should be graded for 10 marks depending on the parameters as analysis, design, application, AI technique and outcome for selected problem statement.

b) Open book test: 05 Marks

c) Regularity and active participation :05 Marks

2. Mid Semester Examination (30 Marks)

Mid semester examination will be based on 40% to 50% syllabus.

B. END SEMESTER EXAMINATION (50 MARKS)

End Semester Examination will be based on syllabus coverage up to the Mid Semester Examination (MSE) carrying 20% to 30% weightage, and the syllabus covered from MSE to ESE carrying 70% to 80% weightage.

Course Type	Course Code	Course Name	Credits
HMP	HMPXX801	Honours/Minor Mini Project	02

Program Outcomes addressed:

1. PO1 : Engineering knowledge
2. PO2 : Problem Analysis
3. PO3 : Design/Development of Solutions
4. PO4 : Conduct investigations of complex problems
5. PO5 : Modern Tool Usage
6. PO6 : The Engineer & World
7. PO7 : Ethics
8. PO8 : Individual & team work
9. PO9 : Communication
10. PO10: Project Management & Finance
11. PO11: Life-long learning

Course Objectives

1. To guide students in identifying specialization-domain problems
2.. To explore advanced solutions using emerging technologies and specialized tools.
3. To develop research aptitude, innovation mindset, entrepreneurship potential, and lifelong learning skills.
4.. To foster self-directed learning, domain-specific competency, and collaboration.

Course Outcomes

At the end of the course, students will be able to:

CO1: Identify and articulate a domain-relevant societal, industrial, or research problem using literature review and analysis.

CO2: Apply engineering principles and specialized tools to design innovative and feasible technical solutions.

CO3: Conduct investigations, simulations, or experiments to validate the proposed solution using appropriate methods.

CO4: Evaluate the solution considering sustainability, ethics, feasibility, and potential for commercialization or IP.

CO5: Demonstrate teamwork, project management, and professional technical communication through reports and presentations.

CO6: Engage in self-directed learning and continuous improvement to enhance domain expertise and professional growth.

Guidelines for the Mini Project

• Projects should align with the Honors/Minor specialization domain

Mini project may be carried out in one or more form of following:

Product preparations, prototype development model, fabrication of set-ups, laboratory experiment development, process modification/development, simulation, software development, integration of software (frontend-backend) and hardware, statistical data analysis, creating awareness in society/environment etc.

- Students must form groups of 3 to 4 members.
- Groups should conduct surveys to identify needs and develop problem statements in consultation with faculty.
- An implementation plan in Gantt/PERT/CPM chart format covering weekly activities must be submitted.
- Each group must maintain a logbook to record weekly progress, to be verified by the faculty supervisor.
- Faculty input should emphasize guiding by faculty and self-learning by group members.
- Groups should propose multiple solutions, select the best one in consultation with the supervisor, and develop a working model.
- The solution to be validated with proper justification and report to be compiled in standard format of the Institute. Software requirement specification (SRS) documents, research papers, competition certificates may be submitted as part of annexure to the report.
- With the focus on self-learning, innovation, research orientation, addressing societal and industry challenges, and developing entrepreneurship qualities among students, the Mini Project should reflect appropriate depth, technical sophistication, specialization-domain relevance, and quality. Students are encouraged to adopt an innovative approach, explore emerging technologies**,** and demonstrate prototype development, domain-specific research outputs, or commercialization potential**,** rather than limiting to basic model implementation.

In-Semester Continuous Assessment and End-Semester Examination Guidelines

- The coordinating Head of the Department will assign a guide to each of the mini-projects and shall form a progress monitoring committee. The guide will carry out weekly monitoring of the project's progress. The committee shall carry out in-semester project evaluation based on presentations with a minimum of two evaluations in a semester.
- Assessment will be based on individual contributions, understanding, and responses to questions asked.
- **Continuous Assessment marks distribution (50 marks):**
    - 20 marks for the Topic Approval Presentation in front of the progress monitoring committee
    - 20 marks for the Mid-Semester Progress Presentation in front of the progress monitoring committee
    - 10 marks for regularity & active participation

The review/progress monitoring committee will assess projects based on the following criteria.

- Theoretical solution completion, including component/system selection/design of software solution and cost analysis.
- Two reviews will occur:
    - The first review will focus on finalizing the problem statement (topic approval).
    - Second review will assess the progress of building a working prototype. (Mid Semester Presentation)

In addition to above mentioned points, the following performance criteria shall be included during in-semester continuous assessment:

1. Quality of survey and need identification aligned with specialization or societal/industry relevance.

2. Clarity and innovativeness in problem definition and solution Clarity, originality, and innovativeness in problem definition, solution approach, and use of advanced tools/techniques.
3. Requirement gathering via SRS/feasibility study, cost-effectiveness, and societal impact of proposed solutions.
4. Completeness and full functioning of the working model.
5. Effective use of skill sets and engineering norms.
6. Verification & validation of the solutions/test cases.
7. Individual contributions to the group.
8. Clarity in written and oral communication.
9. Participation in research paper presentation, domain-specific competitions, hackathons, demonstrations, start-up pitching, or innovation challenges.

End-Semester Examination (50 marks):

1. Presentation and demonstration to internal and external examiners: 20 marks.
2. Emphasis on problem clarity, innovativeness, societal impact, functioning of the model, skill utilization, and communication clarity: 30 marks**.**