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 B. Tech Information Technology

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

Revision: 2024

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) Data Science
b) Cyber Security

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

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
Data Science	1. Computer Engineering 2. Electronics & Telecommunication Engineering 3. Information Technology	1. Mechanical Engineering 2.Electrical Engineering
Cyber Security		

a) 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	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.* **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)*	**10-12**
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.*** **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	**06-08**

	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 clinicians. Data-driven decision-making opens up new avenues for improving healthcare.	**01**

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** ***Learning Objective:***	**06-08**

	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.

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**

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**	**03-05**
	Learning Objectives: *To understand the relevant security implementation with implementation of the newer technologies.*	
	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 of managerial, technical, and physical controls for physical access and environmental 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**	**06-08**
	Learning Objective: *To make learner is understand mobile device security, encompassing wireless threat mitigation and device security considering different wireless infrastructures.*	
	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,	**08-10**

	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: *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.