Course Title: Secure Software Design and Enterprise Computing Lab							
Course Code: MCSELAK124					Examination Scheme		
Total Number of Lecture Hours: 50					External	36	
					Internal	14	
Lecture (L)	0	Practical (P)	4	Tutorial (T)	0	Total Credits	2

Course Objectives

This course aims to equip students with a deep understanding of secure software development, system design, and network services management. Through a series of hands-on experiments, students will learn to identify and analyze software vulnerabilities, implement secure coding practices, and apply security design principles in building robust enterprise applications. Emphasis is placed on ensuring secure coding techniques, defending against common attacks, and managing server resources effectively.

List of Experiments

1. Identifying and Analyzing Software Vulnerabilities
2. Implementing Secure Coding Practices
3. Security Testing and Quality Assurance
4. Security Design Principles
5. Designing a Distributed N-Tier Application
6. Database Design for Enterprise Applications
7. Developing Components in an Enterprise System
8. Implementing and Integrating Enterprise Application Services
9. Presenting a Multi-Tier Software Solution
10. Designing and Implementing a Directory-Based Server Infrastructure
11. Monitoring Server Resources for Availability and Reliability
12. Installing and Administering Network Services
13. Web and Email Server Setup
14. Managing and Troubleshooting Network Services
15. Preventing SQL Injection Attacks
16. Defending Web Applications from Common Attacks
17. Handling Insecure Exceptions and Error Messages
18. Secure Mobile Application Development
19. Web Application Security Testing and Mitigation

Course Outcomes:

1. *Analyze and identify software vulnerabilities, applying secure coding practices to prevent common security risks.*
2. *Design and implement secure enterprise applications, including distributed multi-tier systems and integrating application services with a focus on security.*
3. *Manage network services, monitor server resources for availability and reliability, and ensure secure configuration of servers and network services.*
4. *Test and mitigate security vulnerabilities in web applications and mobile applications, focusing on defending against SQL injections and other common attacks.*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	3	2	2	3	1	-	2	1	1	-	1
2	3	2	3	1	3	2	1	2	2	2	1	2
3	2	2	2	1	3	1	-	2	1	1	-	1
4	2	3	2	2	3	1	-	3	1	2	-	1

Course Title: Biometrics Lab							
Course Code: MCSELAL124					Examination Scheme		
Total Number of Lecture Hours: 50					External	36	
					Internal	14	
Lecture (L)	0	Practical (P)	4	Tutorial (T)	0	Total Credits	2

Course Objectives: *The aim of the course is to provide hands-on experience with various biometric modalities and system components, enable to develop skills in capturing, processing, feature extraction, matching, and evaluation of biometric data.*

List of Experiments

1. Demonstration of basic biometric system components: sensor, feature extractor, matcher, database, decision module.
2. Capturing, pre-processing, and matching fingerprints.
3. Study of fingerprint feature extraction (minutiae detection).
4. Implement face detection and recognition using OpenCV or similar tools.
5. Feature extraction using Eigenfaces or Local Binary Patterns (LBP).
6. Implement a basic iris matching algorithm.
7. Voice verification using dynamic time warping (DTW).
8. Capture palmprints and extract region of interest (ROI) features.
9. Calculate and interpret False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER) for a given biometric system.
10. Apply basic statistical techniques (mean, standard deviation, ROC curves) on biometric datasets.

**This is only a suggested list of experiments/simulations. The instructor is encouraged to familiarize students with additional relevant exercises.*

Recommended Books:

Course Outcomes:

1. *Understand various biometric modalities (fingerprint, face, iris, voice, hand geometry, palmprint, and signature) through practical implementation and feature extraction techniques.*
2. *Evaluate biometric authentication systems by applying matching algorithms and analyzing performance metrics like FAR, FRR, and EER.*
3. *Apply statistical analysis and database management techniques for storing, securing, and interpreting biometric data.*
4. *Address real-world authentication and security challenges in sectors such as, healthcare and government.*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	2	2	3	1	-	1	1	1	-	2
2	3	3	2	3	3	1	-	2	1	1	-	2
3	3	3	2	2	2	2	1	2	1	1	1	2
4	2	2	3	2	2	3	2	3	2	2	1	2

Course Title: Next Generation Networks Lab							
Course Code: MCSELAM124					Examination Scheme		
Total Number of Practical Hours: 48					External	36	
					Internal	14	
Lecture (L)	0	Practical (P)	4	Tutorial (T)	0	Total Credits	2

Course Objectives

To introduce the fundamental concepts relevant to internetworking, design issues, simulations and performance evaluation of different protocols under diverse scenarios.

List of Experiments

1. Introduction to Network Simulators.
2. Experimental study of various protocols operating at diverse layers using packet sniffers.
3. Experiments with packet sniffers to study the behaviour of various protocols.
4. Introduction to NS2 or NS3, small simulation exercises in NS2 or NS3.
5. Experiments in network simulators to study various protocols
6. Setting up IP networks and evaluation of QoS in different situations.
7. Socket programming in high level languages.
8. Introduction of SDN Controllers and mininet.

This is only a suggested list of experiments/simulations. The instructor is encouraged to familiarize students with additional relevant exercises.

Course Learning Outcomes:

1. *CLO1: Demonstrate the use of network simulators (NS2/NS3), packet sniffers, and SDN tools (Mininet, Controllers) for studying network protocols. (Apply, Understand)*
2. *CLO2: Analyze the behavior and performance of protocols across different network layers using simulation and traffic monitoring tools. (Analyze, Evaluate)*
3. *CLO3: Implement socket programming and simulation exercises to understand communication and Quality of Service (QoS) in IP networks. (Apply, Analyze)*
4. *CLO4: Design and evaluate networking experiments/projects integrating simulators, QoS measurements, and SDN concepts for next-generation networking challenges. (Apply, Create, Evaluate)*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	2	2	3	–	–	–	–	–	–	2
2	3	3	2	3	3	–	–	–	–	1	–	2
3	3	2	2	2	3	–	–	–	–	–	–	2
4	3	3	3	3	3	–	–	1	3	3	2	3

Course Title: Graph Theory Lab												
Course Code: MCSELAN124								**Examination Scheme**				
Total Number of Lecture Hours: 50								**External**		**36**		
								Internal		**14**		
Lecture (L)	**0**	**Practical (P)**	**4**	**Tutorial (T)**		**0**	**Total Credits**					**2**

Course Objectives

1. *To provide hands-on experience in implementing basic graph data structures and traversal algorithms.*
2. *To apply graph theory algorithms to real-world applications such as network analysis and optimization.*
3. *To understand graph properties and problem-solving through programming exercises.*
4. *To enable analysis of large graphs using tools like NetworkX, Gephi, or similar.*

List of Experiments

1. Implement graph representations: adjacency matrix and adjacency list.
2. Write a program for Depth First Search (DFS) and Breadth First Search (BFS).
3. Detect cycles in undirected and directed graphs.
4. Implement Prim's and Kruskal's algorithms for Minimum Spanning Tree.
5. Implement Dijkstra's and Bellman-Ford algorithms for shortest path.
6. Check if a graph is bipartite using BFS.
7. Solve the graph coloring problem using backtracking or greedy algorithm.
8. Implement Floyd-Warshall algorithm for all-pairs shortest paths.
9. Implement Ford-Fulkerson algorithm for Maximum Flow in a network.
10. Implement matching algorithms in bipartite graphs (e.g., Hungarian Algorithm).

This is only a suggested list of experiments/simulations. The instructor is encouraged to familiarize students with additional relevant exercises.

Course Outcomes:

1. *Develop and implement graph data structures and traversal algorithms.*
2. *Apply graph algorithms to solve optimization and network problems.*
3. *Analyze and interpret graph properties using programming and tools.*
4. *Utilize graph theory for practical, real-world data analysis.*

Level of CLO-PLO Mapping

CLOs	POs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	3	2	2	0	0	0	0	0	0	1
2	3	3	3	3	2	1	0	0	0	1	0	2
3	3	3	3	3	3	0	0	1	1	1	0	2
4	3	3	3	3	3	1	1	1	1	2	1	3

PROGRAM ELECTIVE-III & IV

Course Title: Data Visualisation							
Course Code: MCSEDAA224					Examination Scheme		
Total Number of Lecture Hours: 50					External	72	
					Internal	28	
Lecture (L)	4	Practical (P)	0	Tutorial (T)	0	Total Credits	4

Course Objectives

- *To introduce fundamental principles of visual perception, Gestalt laws, and their role in visualization design and interpretation.*
- *To develop skills in designing, implementing, and evaluating effective data visualizations, with emphasis on visual mapping, interaction, and minimizing information overload.*
- *To provide techniques for visualizing complex data types, including volumetric, vector, and geographic information.*
- *To familiarize students with emerging trends, technologies, and innovations in data visualization.*

Course Content	No. of Teaching Hours
UNIT 1	**10 Hrs**

Introduction to Visual Perception and Data Representation

Visual perception fundamentals, Gestalt principles, challenges of information overload, methods of visual data representation, visualization reference models, visual mappings, visual analytics, and design of visualization applications.

UNIT 2	**12 Hrs**

Visualization Systems, Interaction Techniques, and Data Types

Classification of visualization systems, interaction techniques (filtering, zooming, linking, brushing), visualization of one-, two-, and multi-dimensional data, text and document visualization, visualization of groups, trees, graphs, clusters, networks, and metaphorical visualization approaches

UNIT 3	**12 Hrs**

Advanced Visualization Techniques

Visualization of volumetric data, vector fields, dynamic processes, and simulations, map and geographic information visualization, GIS systems, collaborative visualization techniques, and evaluation methods for visualizations

UNIT 4	**14 Hrs**

Emerging Trends and Data Structures in Visualization

Recent trends in perception and visualization techniques, data structures for visualization, immersive visualization (AR/VR), real-time visualization technologies, and future directions in data visualization.

Recommended Books:

- *Edward R. Tufte, "The Visual Display of Quantitative Information", Graphics Press, 2001.*
- *Colin Ware, "Information Visualization: Perception for Design", Morgan Kaufmann, 2013.Tamara Munzner, "Visualization Analysis and Design", CRC Press, 2014.*
- *Matthew O. Ward, Georges Grinstein, Daniel Keim, "Interactive Data Visualization: Foundations, Techniques, and Applications", CRC Press, 2015.*
- *Kieran Healy, "Data Visualization: A Practical Introduction", Princeton University Press, 2018.*

Course Learning Outcomes

CLO1: Apply principles of visual perception and Gestalt theory to create meaningful and intuitive visualizations.

CLO2: Design and develop interactive and efficient data visualizations for one-dimensional, multi-dimensional, and complex datasets.

CLO3: Visualize specialized data such as volumetric fields, dynamic processes, and geographic information using appropriate techniques.

CLO4: Analyse and adapt to emerging tools, methods, and trends in the field of data visualization.

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	2	-	2	-	-	-	-	2	-	2
2	3	3	3	2	3	0	0	0	2	2	2	2
3	3	2	3	2	3	-	-	-	1	1	1	2
4	2	2	2	2	3	0	0	0	0	1	0	3

Course Title: Big Data Analytics												
Course Code: MCSEDAB224								Examination Scheme				
Total Number of Lecture Hours: 50								External		72		
								Internal		28		
Lecture (L)	4	Practical (P)	0	Tutorial (T)		0	Total Credits		4			

Course Objectives

1. *To introduce the fundamentals of big data and the challenges in data management.*
2. *To enable students to use the Hadoop ecosystem for distributed data storage and processing.*
3. *To understand big data frameworks such as Apache Spark for real-time processing.*
4. *To analyze structured and unstructured data using big data tools and algorithms.*

Course Content	No. of Teaching Hours
UNIT 1	12 Hrs

Introduction to Big Data

- Introduction to Big Data – Types, Characteristics, and Challenges
- Traditional vs Big Data Approaches; Big Data Applications in Real-world Scenarios
- Introduction to Hadoop Ecosystem – HDFS Architecture, YARN, MapReduce Framework

UNIT 2	12 Hrs

Hadoop and Data Storage

- HDFS Operations, Blocks, Replication; Data Loading using Sqoop and Flume
- Data Querying using Hive and Pig; Hands-on MapReduce Programming – Word Count, Sorting, Filtering

UNIT 3	12 Hrs

Apache Spark and Real-time Processing

- Spark Architecture – RDDs, DAGs, Lazy Evaluation; Spark Core and SQL
- Spark Streaming and Kafka Integration; Performance Tuning and Monitoring in Spark

UNIT 4	14 Hrs

Advanced Big Data Analytics

- Graph Processing with GraphX; Machine Learning with Spark MLlib
- Text and Sentiment Analysis; Case Studies: Recommendation Systems, Social Media Mining

Books:

1. Tom White, *Hadoop: The Definitive Guide*, O'Reilly Media
2. Vignesh Prajapati, *Big Data Analytics with R and Hadoop*, Packt
3. Matei Zaharia, *Learning Spark: Lightning-Fast Big Data Analysis*, O'Reilly
4. Jure Leskovec, Anand Rajaraman, *Mining of Massive Datasets*, Cambridge University Press
5. Boris Lublinsky et al., *Professional Hadoop Solutions*, Wiley

Course Learning Outcomes

After completing this course, the students will be able to:

1. *Explain the fundamental concepts of big data and challenges in handling it.*
2. *Implement Hadoop-based storage and MapReduce-based processing.*
3. *Analyze large-scale data using Spark for real-time and batch processing.*
4. *Apply big data techniques for analytics on structured and unstructured data.*
5. *Evaluate performance of big data solutions in terms of scalability and efficiency.*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	2	1	1	1	1	-	-	-	-	1
2	3	3	2	2	3	1	1	-	-	-	-	2
3	3	3	3	2	3	1	1	-	-	1	-	3
4	3	3	3	3	3	1	1	-	-	2	1	3
5	2	3	3	2	3	1	-	-	-	2	1	3

Course Title: Data Warehouse and Data Mining												
Course Code: MCSEDAC224									Examination Scheme			
Total Number of Leeture Hours: 48									External		72	
									Internal		28	
Lecture (L)	4	Practical (P)	0	Tutorial (T)		0	Total Credits	4				

Course Objectives

1. *To understand the concepts, architecture, and applications of Data Warehousing.*
2. *To explore the techniques and tools of Data Mining for knowledge discovery.*
3. *To learn methods for data preprocessing, transformation, and visualization.*
4. *To analyze and implement classification, clustering, and association rule mining algorithms.*
5. *To evaluate mining results using different metrics and visualization techniques.*

Course Content	No. of Teaching Hours
UNIT 1	**10 Hrs**
• Introduction to Data Warehousing • Architecture and Components. Data Modeling and Star, Snowflake Schemas • ETL Processes, OLAP: Concepts, Types and Operations	
UNIT 2	**12 Hrs**
• Data Cleaning, Integration, Transformation, and Reduction • Discretization and Concept Hierarchy Generation • Association Rule Mining: Apriori, FP-Growth Algorithms • Evaluation of Association Patterns	
UNIT 3	**12 Hrs**
• Classification: Decision Tree, Naive Bayes, k-NN, SVM • Prediction Techniques: Linear & Logistic Regression • Model Evaluation Techniques: Confusion Matrix, Precision, Recall, F1-Score	
UNIT 4	**14 Hrs**
• Clustering: k-Means, Hierarchical Clustering, DBSCAN • Outlier Detection and Anomaly Mining • Web Mining, Text Mining, Applications of Data Mining in Business and Scientific Domains	

Books:

1. **"Data Mining: Concepts and Techniques"**, Jiawei Han, Micheline Kamber, Jian Pei 3rd Edition, Morgan Kaufmann
2. **"Data Warehousing Fundamentals"**, Paulraj Ponniah, Wiley
3. **"Mastering Data Mining"**, Michael J. Berry, Gordon S. Linoff, Wiley
4. **"Building the Data Warehouse"**, W.H. Inmon, Wiley
5. **"Introduction to Data Mining"**, Pang-Ning Tan, M. Steinbach, V. Kumar, Pearson Education

Course Outcomes:

After successful completion of the course, the students will be able to:

1. *Understand the architecture and components of data warehouses*
2. *Apply data preprocessing and transformation techniques for data mining*
3. *Analyze and implement classification, clustering, and association algorithms*
4. *Evaluate the results of data mining using appropriate metrics*
5. *Apply mining techniques to real-world datasets using appropriate tools*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	-	-	-	-	-	-	-	-	-	-
2	3	3	2	-	-	-	-	-	-	-	-	-
3	3	3	3	2	-	-	-	-	-	-	-	-
4	2	3	3	-	-	-	-	-	-	-	-	-
5	3	3	3	3	2	-	-	-	2	2		2

Course Title: Data Security & Access Control									
Course Code: MCSEDAD224							Examination Scheme		
Total Number of Lecture Hours: 48							External	72	
							Internal	28	
Lecture (L)	4	Practical (P)	0	Tutorial (T)		0	Total Credits		4

Course Objectives

- *The objective of the course is to provide fundamentals of access control techniques along with application areas of access control techniques.*
- *Analyse the structure and application of RBAC models and compare them with DAC and MAC access control policies.*
- *Examine integrity and security models while integrating RBAC into enterprise IT infrastructures. Explore smart card technology, its security mechanisms, and emerging trends in data security management.*

Course Content	No. of Teaching Hours
UNIT 1	**10 Hrs**
Introduction to Access Control, Purpose and fundamentals of access control, brief history, Policies of Access Control, Models of Access Control, and Mechanisms, Recent trends in access control mechanisms, Discretionary Access Control (DAC), Non- Discretionary Access Control, Mandatory Access Control (MAC). Capabilities and Limitations of Access Control Mechanisms: Access Control List (ACL) and Limitations, Capability List and Limitations.	
UNIT 2	**12 Hrs**
Role-Based Access Control (RBAC) and Limitations, Core RBAC, Hierarchical RBAC, Statically Constrained RBAC, Dynamically Constrained RBAC, Limitations of RBAC. Comparing RBAC to DAC and MAC Access control policy. Case study of Role-Based Access Control (RBAC) systems.	
UNIT 3	**12 Hrs**
Biba's integrity model, Clark-Wilson model, Domain type enforcement model, mapping the enterprise view to the system view, Role hierarchies- inheritance schemes, hierarchy structures and inheritance forms, using SoD in real system Temporal Constraints in RBAC, MAC AND DAC. Integrating RBAC with enterprise IT infrastructures: RBAC for WFMSs, RBAC for UNIX and JAVA environments Case study: Multi-line Insurance Company.	
UNIT 4	**14 Hrs**
Smart Card based Information Security, Smart card operating system fundamentals, design and implantation principles, memory organization, smart card files, file management, atomic operation, smart card data transmission ATR, PPS Security techniques- user identification, smart card security, quality assurance and testing, smart card life cycle-5 phases, smart card terminals. Recent Trends related to data security management, vulnerabilities in different DBMS.	

Recommended Books:

1. *Computer Security: Principles and Practice" (4th Edition) by William Stallings and Lawrie Brown*
2. *Role Based Access Control: David F. Ferraiolo, D. Richard Kuhn, Ramaswamy Chandramouli. Second Edition*

Course Learning Outcomes

CLO1: In this course, the students will be enabled to understand and implement classical models and algorithms

CLO2: They will learn how to analyse the data, identify the problems, and choose the relevant models and algorithms to apply.

CLO3: They will learn how to analyse the data, identify the problems, and choose the relevant models and algorithms to apply.

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	2	1	2	1	1	0	0	1	0	1
2	2	3	3	2	2	1	1	0	0	1	0	1
3	2	3	3	2	2	1	1	0	0	1	0	1

Course Title: Web Analytics & Development							
Course Code: MCSEDAE224					**Examination Scheme**		
Total Number of Lecture Hours: 48					**External**	72	
					Internal	28	
Lecture (L)	4	**Practical (P)**	0	**Tutorial (T)**	0	**Total Credits**	4

Course Objectives

1. *To provide an in-depth understanding of web analytics tools, methodologies, and metrics.*
2. *To enable students to design and develop interactive, dynamic, and analytics-enabled web applications.*
3. *To integrate analytical insights into web development for optimizing user experience and digital marketing.*
4. *To develop the capability to extract actionable insights from web data to support decision-making.*

Course Content	No. of Teaching Hours
UNIT 1	**12 Hrs**
Web Fundamentals and Development Basics HTML5, CSS3, JavaScript, Responsive Design, Client-server architecture, HTTP, HTTPS, and protocols, Introduction to Content Management Systems (CMS).	
UNIT 2	**12 Hrs**
Server-side Development & Databases Introduction to backend frameworks (e.g., Node.js/PHP/Python), Connecting to Databases (MySQL, MongoDB), RESTful APIs and Web Services	
UNIT 3	**12 Hrs**
Web Analytics Concepts Introduction to Web Analytics: Definitions, Benefits, Tools, Key Metrics: Page views, sessions, bounce rate, conversions, Google Analytics: Account setup, goals, dashboards, Traffic sources, audience demographics, behaviour analysis.	
UNIT 4	**12 Hrs**
Advanced Web Analytics & Optimization Campaign Tracking: UTM parameters, Email/Ad campaign analysis, A/B Testing and Multivariate Testing, SEO basics, Keyword Analysis, Google Search Console, Heatmaps and Clickstream Analysis	

Recommended Books:

1. *Justin Cutroni,* Google Analytics, *O'Reilly Media.*
2. *Avinash Kaushik,* Web Analytics 2.0, *Sybex.*
3. *Jon Duckett,* HTML and CSS: Design and Build Websites, *Wiley.*
4. *Robin Nixon,* Learning PHP, MySQL & JavaScript, *O'Reilly.*

Course Learning Outcomes

1. *Understand fundamental concepts, key tools, and metrics of web analytics.*
2. *Apply web development techniques and integrate analytics solutions into websites.*
3. *Analyze web traffic data and generate actionable insights for business improvement.*
4. *Develop analytics-driven web applications and conduct user behavior analysis.*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	2	1	2	1	0	0	0	1	0	1
2	2	3	3	2	2	1	0	0	0	2	0	1
3	2	3	3	2	2	1	0	0	0	1	0	2
4	2	2	3	2	3	1	0	0	0	1	0	2

Course Title: Knowledge Discovery							
Course Code: MCSEDAI224					Examination Scheme		
Total Number of Lecture Hours: 48					External	72	
					Internal	28	
Lecture (L)	4	Practical (P)	0	Tutorial (T)	0	Total Credits	4

Course Objectives

1. *To introduce the concepts and techniques of data mining and knowledge discovery.*
2. *To impart knowledge about preprocessing, cleaning, and transformation of data for mining tasks.*
3. *To develop skills in various data mining techniques such as classification, clustering, and association rule mining.*
4. *To enable students to analyze real-world data using advanced tools and interpret the discovered knowledge.*

Course Content	No. of Teaching Hours
UNIT 1	**10 Hrs**
Introduction and Preprocessing Introduction to KDD process, Difference between data mining and knowledge discovery, Types of data and patterns, Data preprocessing: data cleaning, integration, reduction, transformation, Data warehousing: OLAP, data cube technology	
UNIT 2	**12 Hrs**
Classification and Prediction Basic concepts, decision tree induction, Bayesian classification, Rule-based classification, model evaluation and performance metrics, Techniques: k-nearest neighbor, SVM, ensemble methods (bagging, boosting), Predictive modeling and regression techniques	
UNIT 3	**12 Hrs**
Clustering and Association Analysis Cluster analysis: Partitioning methods, hierarchical methods, density-based methods, Evaluation of clustering techniques, Association rule mining: Apriori algorithm, FP-Growth algorithm, Interestingness measures and constraint-based mining	
UNIT 4	**14 Hrs**
Advanced Topics and Applications Web mining, spatial mining, text and multimedia mining, Mining social network data, Privacy preserving data mining, Case studies in retail, health, finance, and bioinformatics	

Recommended Books:

1. *Jiawei Han, Micheline Kamber, and Jian Pei, "Data Mining: Concepts and Techniques," Morgan Kaufmann.*
2. *Pang-Ning Tan, Michael Steinbach, and Vipin Kumar, "Introduction to Data Mining," Pearson.*
3. *Arun K. Pujari, "Data Mining Techniques," Universities Press.*
4. *Ian H. Witten, Eibe Frank, and Mark A. Hall, "Data Mining: Practical Machine Learning Tools and Techniques," Morgan Kaufmann.*

Course Learning Outcomes

1. *Understand the foundational concepts of data mining and knowledge discovery processes.*
2. *Apply data preprocessing techniques to prepare data for analysis.*
3. *Design and implement data mining algorithms for classification, clustering, and association rule mining.*
4. *Evaluate and interpret the results from real-world data mining applications*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	1	2	1	-	-	-	-	-	-	-
2	3	3	2	2	2	-	-	-	-	-	-	-
3	3	3	3	2	3	-	-	-	-	-	-	-
4	3	2	2	3	2	1	-	-	-	-	-	-

Course Title: Introduction to Deep Learning							
Course Code: MCSEDAG224					Examination Scheme		
Total Number of Lecture Hours: 48					External	72	
					Internal	28	
Lecture (L)	4	Practical (P)	0	Tutorial (T)	0	Total Credits	4

Course Objectives

To present the mathematical, statistical and computational challenges of building neural networks and study the concepts of deep learning to enable the students to know deep learning techniques to support real-time applications and examine the case studies of deep learning techniques.

Course Content	No. of Teaching Hours
UNIT 1	**12 Hrs**
Principles of ANN design, Basic network structure, Perceptron's input-output principles, Feedforward neural networks - deep model, Output units and hidden units. Backpropagation algorithm: Gradient Descent (GD), Momentum-based GD, Nesterov Accelerated GD, Stochastic GD. Vanishing gradient problem, New optimization methods: Adagrad, Adadelta, RMSprop, Adam	
UNIT 2	**12 Hrs**
Training deep models: Hyperparameters and validation sets, Cross-validation, Overfitting and underfitting, Bias vs variance trade-off. Regularization methods: Dropout, Batch Normalization, Early stopping Autoencoders and relation to PCA, Regularization in autoencoders, Denoising autoencoders, Sparse autoencoders, Greedy Layerwise Pre-training, Better activation functions & weight initialization methods, Batch Normalization	
UNIT 3	**12 Hrs**
Convolution operation, Pooling layers, Regularization in CNNs, Architectural overview of CNNs, Layers, filters, parameter sharing. Popular CNN architectures: AlexNet, VGGNet, GoogleNet, ResNet	
UNIT 4	**12 Hrs**
Sequence learning with neural networks, Unrolling the recurrence, Training RNNs - Backpropagation Through Time (BPTT), Long Short-Term Memory (LSTM), Bidirectional LSTM, Gated Recurrent Units (GRU). Encoder-decoder sequence-to-sequence architecture, Attention mechanism, Attention mechanism over images. Introduction to unsupervised training of neural networks: Restricted Boltzmann Machines.	

Recommended Books:

1. Deng & Yu, Deep Learning: Methods and Applications, Now Publishers, 2013.
2. Ian Goodfellow, Yoshua Bengio, Aaron Courville, Deep Learning, MIT Press, 2016.
3. Michael Nielsen, Neural Networks and Deep Learning, Determination Press, 2015.
4. Hands–On Machine Learning with Scikit–Learn and TensorFlow 2e: Concepts, Tools, and Techniques to Build Intelligent Systems by Aurelien Geron

Course Learning Outcomes:

1. *Explain the fundamental concepts of artificial neural networks (ANNs), including perceptrons, feedforward networks, backpropagation, and optimization techniques such as gradient descent and Adam optimizer.*
2. *Apply deep learning techniques such as dropout, batch normalization, and regularization to design, train, and optimize neural network models while addressing issues like overfitting, vanishing gradients, and hyperparameter tuning.*
3. *Analyze and implement various deep learning architectures including CNNs and RNNs (LSTM, GRU), attention mechanisms, and encoder-decoder models for tasks involving images, sequences, and time-series data.*
4. *Evaluate machine learning models using cross-validation, ensemble methods, and clustering algorithms, and demonstrate understanding of advanced topics like reinforcement learning, PCA, generative models, and Bayesian inference.*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	2	1	2	-	-	-	1	1	0	2
2	3	3	3	2	2	1	-	-	1	1	1	2
3	3	3	3	2	3	1	-	-	1	1	1	2
4	3	3	2	3	3	1	1	1	1	2	2	2

Course Title: Pattern Recognition							
Course Code: MCSEDAH224						Examination Scheme	
Total Number of Lecture Hours: 48						External	72
						Internal	28
Lecture (L)	4	Practical (P)	0	Tutorial (T)	0	Total Credits	4

Course Objectives

- *To introduce basic concepts of probability, random processes, and linear algebra relevant to pattern recognition.*
- *To study Bayes decision theory and statistical methods for parameter estimation.*
- *To understand clustering, unsupervised learning techniques, and sequential pattern recognition models like HMMs.*
- *To explore dimensionality reduction techniques, discriminant functions, and non-metric classification methods.*

Course Content	No. of Teaching Hours
UNIT 1	**12 Hrs**
Basics of Probability, Random Processes and Linear Algebra: Probability: independence of events, conditional and joint probability, Bayes' theorem; Random Processes: Stationary and non-stationary processes, Expectation, Autocorrelation, Cross-Correlation, spectra; Linear Algebra: Inner product, outer product, inverses, eigen values, eigen vectors.	
UNIT 2	**12 Hrs**
Bayes Decision Theory: Minimum-error-rate classification, Classifiers, Discriminant functions, Decision surfaces, Normal density and discriminant functions, discrete features Parameter Estimation Methods: Maximum-Likelihood estimation: Gaussian case; Maximum a Posteriori estimation; Bayesian estimation: Gaussian case	
UNIT 3	**12 Hrs**
Unsupervised learning and clustering: Criterion functions for clustering; Algorithms for clustering: K-Means, Hierarchical and other methods; Cluster validation; Gaussian mixture models; Expectation-Maximization method for parameter estimation; Maximum entropy estimation Sequential Pattern Recognition: Hidden Markov Models (HMMs); Discrete HMMs; Continuous HMMs Nonparametric techniques for density estimation: Parzen-window method; K-Nearest Neighbour method	
UNIT 4	**12 Hrs**
Dimensionality reduction: Fisher discriminant analysis; Principal component analysis; Factor Analysis Linear discriminant functions: Gradient descent procedures; Perceptron; Support vector machines Non-metric methods for pattern classification: Non-numeric data or nominal data; Decision trees: CART	

Recommended Books:

1. Devi V.S. Murty, M.N. (2011) Pattern Recognition: An Introduction, Universities Press, Hyderabad.
2. R.O. Duda, P.E. Hart and D.G. Stork, Pattern Classification, John Wiley,2001.
3. Statistical Pattern Recognition; K. Fukunaga; AcademicPress,2000.
4. S. Theodoridis and K. Koutroumbas, Pattern Recognition, 4thEd., AcademicPress,2009.

Course Learning Outcomes:

1. *Understand fundamental concepts of probability, random processes, and linear algebra for pattern recognition tasks.*
2. *Apply Bayes Decision Theory and statistical parameter estimation for designing classifiers.*
3. *Design and implement clustering algorithms, Hidden Markov Models (HMMs), and nonparametric density estimation methods.*
4. *Apply dimensionality reduction techniques and construct classifiers using linear and non-metric methods like decision trees and SVMs.*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	2	2	2	1	1	1	1	1	1	2
2	3	3	3	2	3	1	1	1	2	1	1	2
3	3	3	3	3	3	2	2	1	2	1	1	3
4	3	3	3	3	3	2	2	1	2	2	1	3

Course Title: Intrusion Detection												
Course Code: MCSEDAI224								Examination Scheme				
Total Number of Lecture Hours: 50								External		72		
								Internal		28		
Lecture (L)	4	Practical (P)	0	Tutorial (T)		0	Total Credits		4			

Course Objectives

- *To understand the foundational concepts of computer and network security, including threat landscapes and limitations of security solutions.*
- *To examine various classes of cyber-attacks across network, application, and human layers and understand the different types of attackers.*
- *To explore anomaly detection systems and algorithms, focusing on network and host-based anomaly detection techniques.*
- *To analyze advanced malware detection methods, including attack trees, botnet autopsy, polymorphism, and zero-day threat detection.*

Course Content	No. of Teaching Hours
UNIT 1	**12 Hrs**
The state of threats against computers, and networked systems-Overview of computer security solutions and why they fail-vulnerability assessment, firewalls, VPN's -Overview of Intrusion Detection and Intrusion Prevention	
UNIT 2	**12 Hrs**
Classes of attacks - Network layer: scans, denial of service, -Application layer: software exploits, code injection-Human layer: identity theft, Hesitated groups-Automated: Drones, Worms, Viruses A General IDS model and taxonomy, Signature-based Solutions, Snort, Snort rules, Evaluation of IDS, Cost sensitive IDS	
UNIT 3	**12 Hrs**
Anomaly Detection Systems and Algorithms-Network Behavior Based Anomaly Detectors (rate based)-Host-based Anomaly Detectors-Software Vulnerabilities State transition, Immunology, Payload Anomaly Detection	
UNIT 4	**14 Hrs**
Attack trees and Correlation of alerts-Autopsy of Worms and Botnets-Malware detection-Obfuscation, polymorphism, Email/IM security issues-Viruses/Spam-From signatures to thumbprints to zero day detection-Insider Threat issues-Taxonomy-Masquerade and Impersonation	

Recommended Books:

1. *Crimeware, Understanding New Attacks and Defenses, Markus Jakobsson and Zulfikar Ramzan, Symantec Press, ISBN: 978-0-321-50195-0 2008*
2. *The Art of Computer Virus Research and Defense, Peter Szor, Symantec Press ISBN 0-321 30545-3*

Course Outcomes

- *CLO1: Demonstrate an understanding of the primary threats to computer and network systems and the limitations of current security measures.*
- *CLO2: Identify and classify various types of cyber-attacks and attackers across different layers, including network, application, and human aspects.*
- *CLO3: Apply anomaly detection techniques to recognize abnormal behavior in network and host systems.*
- *CLO4: Analyze and evaluate malware detection strategies, including signature and behavioral-based methods, for defending against advanced and zero-day threats.*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	2	2	1	1	1	1	0	1	0	2
2	3	3	2	2	2	1	1	1	0	1	0	2
3	3	3	3	3	3	1	1	1	0	1	0	3
4	3	3	3	3	3	1	1	1	0	1	1	3

Course Title: Data Encryption & Compression							
Course Code: MCSEDAJ224					Examination Scheme		
Total Number of Lecture Hours: 48					External	72	
					Internal	28	
Lecture (L)	4	Practical (P)	0	Tutorial (T)	0	Total Credits	4

Course Objectives

- Introduce students to the fundamental concepts of encryption, decryption, cryptographic algorithms, and security protocols.
- Teach students how symmetric and asymmetric encryption methods work, and when each is applied in real-world systems.
- Introduce students to hash functions, digital signatures, and their role in data security.
- Provide knowledge about various data compression techniques and how they are used to reduce data size without losing information.
- Understand advanced encryption schemes and modern cryptographic protocols such as RSA, AES, and their usage in secure communication.

Course Content	No. of Teaching Hours
UNIT 1	**12 Hrs**
History of encryption techniques, and the evolution of cryptographic systems. Encryption, decryption, keys, cipher-text, plaintext, cryptanalysis, etc. Types of Cryptographic Systems: Symmetric key encryption, asymmetric key encryption and their applications. Cryptographic Services: Confidentiality, integrity, authentication, and non-repudiation.	
UNIT 2	**12 Hrs**
Overview of Symmetric Encryption: Block ciphers, stream ciphers, key management. Data Encryption Standard (DES): Algorithm design, encryption and decryption, weaknesses of DES. Advanced Encryption Standard (AES): AES algorithm, key expansion, rounds, and its applications in modern cryptography.	
UNIT 3	**12 Hrs**
Public Key Cryptography and Message Authentication: Approaches to Message Authentication, SHA-1, MD5, Public-Key Cryptography Principles, RSA, Hash Function and Digital Signatures, Diffie-Hellman key exchange and its significance. Introduction to Key Management and Distribution, Symmetric key distribution, Public key distribution, X.509 Certificates, Public key Infrastructure. SSL/TLS protocol, HTTPS.	
UNIT 4	**12 Hrs**
Need for data compression, Fundamental concept of data compression & coding, Communication model, Compression ratio, Requirements of data compression, Classification, Basic encoding (Run-Length Encoding), applications in image and text compression. Methods of Data Compression: Data compression-Loss less & Lossy compression.	

Recommended Books:

1. *Stallings, William. Cryptography & Network Security: Principles & Practice. 7th ed., Pearson, 2017.*
2. *Paar, Christof, and Jan Pelzl. Understanding Cryptography: A Textbook for Students and Practitioners. 2nd ed., Springer, 2010.*
3. *Salomon, David. Data Compression: The Complete Reference. 4th ed., Springer, 2007.*

Course Outcomes:

CLO1: Demonstrate an understanding of the core concepts of cryptography, including symmetric and asymmetric encryption, key management, and cryptographic protocols.

CLO2: Understand the concept of hash functions, implement them, and apply them in digital signatures and data integrity checks.

CLO3: Understand and apply cryptographic protocols such as SSL/TLS for secure communication.

CLO4: Use various data compression algorithms like run-length encoding to reduce data size.

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	2	2	2	1	0	1	0	1	0	2
2	3	3	3	3	3	1	0	1	0	1	0	2
3	3	3	3	3	3	1	0	1	1	2	0	2
4	3	2	3	2	3	0	0	0	0	1	0	2

Course Title: Steganography & Digital Watermarking												
Course Code: MCSEDAK224									Examination Scheme			
Total Number of Lecture Hours: 48									External		72	
									Internal		28	
Lecture (L)	4	Practical (P)	0	Tutorial (T)		0	Total Credits	4				

Course Objectives: *The aim of the course is give a comprehensive understanding of the principles, methods, and techniques for securely hiding and detecting information within digital media such as text, images, audio, and video. The course also focuses on steganalysis to detect hidden information and assess system robustness against various attacks.*

Course Content	No. of Teaching Hours
UNIT 1	**12 Hrs**
Steganography: Overview, History, Methods for hiding (text, images, audio, video, speech etc.), Issues: Security, Capacity and Imperceptibility, Steganalysis: Active and Malicious Attackers, Active and passive steganalysis.	
UNIT 2	**12 Hrs**
Frameworks for secret communication (pure Steganography, secret key, public key steganography), Steganography algorithms (adaptive and non-adaptive).	
UNIT 3	**12 Hrs**
Steganography techniques: Substitution systems, Spatial Domain, Transform domain techniques, Spread spectrum, Statistical steganography, Cover Generation and cover selection, Tools: EzStego, FF Encode, Hide 4 PGP, Hide and Seek, S Tools etc.)	
UNIT 4	**12 Hrs**
Detection, Distortion, Techniques: LSB Embedding, LSB Steganalysis using primary sets, Texture based, analyze texture patterns to identify inconsistencies that may indicate hidden data. Intentional distortion, detection of distortion.	

Recommended Books:

1. *Peter Wayner, Disappearing Cryptography–Information Hiding: Steganography & Watermarking", Morgan Kaufmann Publishers, New York, 2002.*
2. *Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, TonKalker, Digital Watermarking & Steganography", Margan Kaufmann Publishers, New York, 2008.*
3. *Information Hiding: Steganography and Watermarking-Attacks and Countermeasures by Neil F. Johnson, ZoranDuric, SushilJajodia*
4. *Information Hiding Techniques for Steganography and Digital Watermarking by Stefan Katzenbeisser, Fabien A. P. Petitcolas.*

Course Outcomes:

1. *Understand the fundamental principles of steganography and steganalysis, including historical development, methods for hiding information across different media and issues related to security, capacity, and imperceptibility.*
2. *Analyze and apply different frameworks and algorithms for secret communication, including pure steganography, secret key, and public key methods.*
3. *Design and implement steganographic systems using substitution systems, spatial and transform domain techniques, spread spectrum, and statistical methods.*
4. *Evaluate and detect hidden information by applying advanced detection methods such as LSB embedding and steganalysis using primary sets and texture-based analysis, and assess the robustness of steganographic systems under distortion attacks.*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	1	1	2	1	-	2	-	1	-	2
2	3	3	2	2	2	1	-	2	-	1	-	2
3	3	2	3	2	3	1	-	2	1	2	1	2
4	2	3	2	3	2	1	1	3	1	2	-	2

Course Title: Information Theory and Coding									
Course Code: MCSEDAL224							Examination Scheme		
Total Number of Lecture Hours: 50							External	72	
							Internal	28	
Lecture (L)	4	Practical (P)	0	Tutorial (T)		0	Total Credits	4	

Course Objectives

- ***Fundamentals of Information Theory***: *To introduce the foundational principles of information theory, including entropy, mutual information, and Shannon's theorems, and to understand their relevance in communication systems.*
- ***Source and Channel Coding***: *To develop a deep understanding of source coding for data compression and channel coding for error detection and correction, exploring both theoretical concepts and practical implementations.*
- ***Error Correction and Coding Techniques***: *To explore coding schemes, and their applications.*
- ***Applications of Information Theory***: *To examine the applications of information theory in areas such as cryptography, data compression, wireless communications, and machine learning, emphasizing real-world problem-solving.*

Course Content	No. of Teaching Hours
UNIT 1	**12 Hrs**
Fundamentals of Information Theory, Entropy, Joint and Conditional Entropy, Mutual Information, Shannon's Theorems, Information Channels, Channel Capacity	
UNIT 2	**12 Hrs**
Lossless Source Coding, Huffman Coding, Arithmetic Coding, Lossy Source Coding, Rate-Distortion Theory	
UNIT 3	**12 Hrs**
Error Detection and Correction Codes, Linear Block Codes, Hamming Codes, Cyclic Codes, Convolutional Codes, Error Detection Codes (Parity, Checksums, CRC).	
UNIT 4	**14 Hrs**
Applications of Information Theory in Cryptography, Data Compression, Wireless Communications, and Machine Learning	

Recommended Books:

1. Elements of Information Theory, Thomas M. Cover and Joy A. Thomas, Wiley-Interscience, ISBN: 978-0-471-24195-9, 2006
2. Information Theory, Inference, and Learning Algorithms, David J.C. MacKay, Cambridge University Press, ISBN: 978-0-521-64298-9, 2003.
3. A First Course in Information Theory, Raymond W. Yeung, Springer, ISBN: 978-0-387-78910-1, 2006
4. Error Control Coding: Fundamentals and Applications, Shu Lin and Daniel J. Costello, Pearson, ISBN: 978-0-13-283796-4, 2004

Course Outcomes

CLO1: Demonstrate a solid understanding of key information theory concepts, including entropy, mutual information, and channel capacity, and apply Shannon's theorems to analyze communication channels.
CLO2: Apply lossless and lossy source coding techniques, such as Huffman and arithmetic coding, to compress data and analyze rate-distortion trade-offs in lossy coding scenarios.
CLO3: Design and implement error-correcting codes, including Hamming, cyclic, and convolutional codes, for effective error detection and correction in communication systems.
CO4: Evaluate and apply information theory principles in cryptography, data compression, wireless communication, and machine learning, effectively addressing real-world problems in these fields

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	3	2	3	2	1	0	1	0	1	0	2
2	3	3	3	3	3	0	0	1	0	1	0	2
3	3	3	3	3	3	0	0	1	1	1	0	2
4	3	3	3	3	3	1	0	1	1	2	1	3

Course Title: Security Assessment & Risk Analysis							
Course Code: MCSEDAM224						Examination Scheme	
Total Number of Lecture Hours: 50						External	72
						Internal	28
Lecture (L)	4	Practical (P)	0	Tutorial (T)	0	Total Credits	4

Course Objectives

- *Describe the concepts of risk management*
- *Define and differentiate various Contingency Planning components*
- *Integrate the IRP, DRP, & BCP plans into a coherent strategy to support sustained organizational operations.*
- *Define and be able to discuss incident response options, and design an Incident Response Plan for sustained organizational operations.*

Course Content	No. of Teaching Hours
UNIT 1 Security Basics and Operation Security	**10 Hrs**
Information Security (INFOSEC) Overview: critical information characteristics – availability information states – processing security counter measures education, training and awareness, critical information characteristics – confidentiality critical information characteristics – integrity, information states – storage, information states – transmission, security counter measures policy, procedures and practices, threats, vulnerabilities. Operations Security (OPSEC): OPSEC surveys/OPSEC planning INFOSEC: computer security – audit, cryptography encryption (e.g., point to point, network, link), cryptography key management (to include electronic key), cryptography strength (e.g., complexity, secrecy, characteristics of the key).	
UNIT 2 Threats to and Vulnerabilities of Systems	**12 Hrs**
Definition of terms (e.g., threats, vulnerabilities, risk), major categories of threats (e.g., fraud, Hostile Intelligence Service (HOIS), malicious logic, hackers, environmental and technological hazards, disgruntled employees, careless employees, HUMINT, and monitoring), threat impact areas, Countermeasures: assessments (e.g., surveys, inspections), Concepts of Risk Management: consequences (e.g., corrective action, risk assessment), cost/benefit analysis of controls, implementation of cost effective controls, monitoring the efficiency and effectiveness of controls (e.g., unauthorized or inadvertent disclosure of information), threat and vulnerability assessment	
UNIT 3 Security Planning	**12 Hrs**
Directives and procedures for policy mechanism, Risk Management: acceptance of risk (accreditation), corrective actions information identification, risk analysis and/or vulnerability assessment components, risk analysis results evaluation, roles and responsibilities of all the players in the risk analysis process, Contingency Planning/Disaster Recovery: agency response procedures and continuity of operations, contingency plan components, determination of backup requirements, development of plans for recovery actions after a disruptive event, development of procedures for offsite processing, emergency destruction procedures, guidelines for determining critical and essential workload, team member responsibilities in responding to an emergency situation	
UNIT 4 Policies and Procedures	**14 Hrs**
Physical Security Measures: alarms, building construction, cabling, communications centre, environmental controls (humidity and air conditioning), filtered power, physical access control systems (key cards, locks and alarms) Personnel Security Practices and Procedures: access authorization/verification (needtoknow), contractors, employee clearances, position sensitivity, security training and awareness, systems maintenance personnel, Administrative Security Procedural Controls: attribution, copyright protection and licensing , Auditing and Monitoring: conducting security reviews, effectiveness of security programs, investigation of security breaches, privacy review of accountability controls, review of audit trails and logs	

Recommended Books:

1. *Security Risk Management: Building an Information Security Risk Management Program, Evan Wheeler, Elsevier, 1st Edition (2011)*
2. *Principles of Incident Response and Disaster Recovery, Whitman & Mattord, Course Technology ISBN: 141883663X*

Course Outcomes

CLO1: Capable of recommending contingency strategies including data backup and recovery and alternate site selection for business resumption planning

CLO2: Skilled to be able to describe the escalation process from incident to disaster in case of security disaster

CLO3: Capable of Designing a Disaster Recovery Plan for sustained organizational operations

CLO4: Capable of Designing a Business Continuity Plan for sustained organizational operations

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	2	2	3	2	2	2	1	1	1	2	2	2
2	2	2	2	2	2	2	1	2	1	2	2	2
3	3	3	3	3	3	2	1	1	1	2	2	3
4	3	3	3	3	3	2	1	1	1	2	3	3

Course Title: Secure Coding												
Course Code: MCSEDAN224								Examination Scheme				
Total Number of Lecture Hours: 48								External		72		
								Internal		28		
Lecture (L)	4	Practical (P)	0	Tutorial (T)		0	Total Credits		4			

Course Objectives

1. *To understand common security vulnerabilities in software and coding practices that lead to them.*
2. *To study secure coding principles, defensive programming, and input validation techniques.*
3. *To explore language-specific vulnerabilities and secure coding practices in C/C++, Java, and Python.*
4. *To introduce threat modeling and secure software development lifecycle (SSDLC).*

Course Content	No. of Teaching Hours
UNIT 1	10 Hrs
Software Security Fundamentals Security in the software lifecycle Common software vulnerabilities: buffer overflows, input validation, command injection, Secure software development practices, Introduction to CWE (Common Weakness Enumeration) and CVE (Common Vulnerabilities and Exposures)	
UNIT 2	12 Hrs
Secure Programming in C/C++ and Java Buffer overflows, stack smashing, integer overflows, Memory safety: use-after-free, double free, Secure coding in Java: avoiding serialization flaws, input validation, Exception handling and secure use of APIs	
UNIT 3	12 Hrs
Web and Database Security Input validation and sanitization, Preventing Cross-site scripting (XSS), Cross-site request forgery (CSRF), and SQL injection, Session management and authentication flaws, Secure file handling and configuration	
UNIT 4	14 Hrs
Secure SDLC and Advanced Topics Threat modeling and risk assessment, Static and dynamic code analysis, Secure design principles and secure code review, Overview of tools: SonarQube, Coverity, Fortify, Case studies of real-world vulnerabilities	

Recommended Books

1. ***"Secure Coding in C and C++"*** *– Robert C. Seacord, Pearson Education*
2. ***"The Web Application Hacker's Handbook"*** *– Dafydd Stuttard, Marcus Pinto*
3. ***"Writing Secure Code"*** *– Michael Howard, David LeBlanc, Microsoft Press*
4. ***"Computer Security: Principles and Practice"*** *– William Stallings and Lawrie Brown*

Course Outcomes

After successful completion of the course, the student will be able to:

1. *Identify common software vulnerabilities and explain how insecure code leads to exploitation.*
2. *Apply secure coding techniques to prevent vulnerabilities such as buffer overflows, XSS, and SQL injection.*
3. *Analyze and refactor insecure code across different programming languages using secure coding standards.*
4. *Design secure software using threat modeling, code review, and secure SDLC practices.*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	3	2	2	2	1	0	2	1	1	0	2
2	3	3	3	2	3	1	0	1	0	1	0	2
3	3	3	3	2	3	1	0	1	0	1	0	2
4	3	3	3	3	3	2	0	2	1			

Course Title: Network Security							
Course Code:MCSEDAO224					Examination Scheme		
Total Number of Lecture Hours: 48					External	54	
					Internal	21	
Lecture (L)	4	Practical (P)	0	Tutorial (T)	0	Total Credits	4

Course Objectives

The aim of this course is to provide background, comprehensive and deep knowledge of security concepts relevant to networks. Introduce the importance of security algorithms (Confidentiality, Integrity, Authentication, etc) in the modern digital world.

Course Content	No. of Teaching Hours
UNIT 1	**12 Hrs**

Introduction to Network Security: security attacks, services and mechanisms.
Basic Concepts: cryptography, steganography, number theory (Concept of Groups, Rings, Fields, GF(p) and GF(p^n), random numbers, Discrete Logarithm Problem and Prime Factorization.
Secret Key Encryption: DES, IDEA, RC4, AES (Rijndael)
Public key encryption: Diffie-Hellman, RSA, ECC

UNIT 2	12 Hrs

Message Authentication Codes: Authentication requirements, authentication functions, message authentication code,
Hash Functions: security of hash functions, birthday attacks, MD5, Secure hash algorithms (SHA-1)
Digital Signatures: Digital Signatures, Elgamal and Schnorr Digital Signature Techniques, Digital signature standards (DSS).

UNIT 3	12 Hrs

Key Management and distribution: Symmetric key distribution, Public key distribution, X.509 Certificates, Public key Infrastructure. Basic concepts in group key management Overview of Group key agreement protocols
Authentication Applications: Kerberos
Electronic mail security: pretty good privacy (PGP), S/MIME.

UNIT 4	12 Hrs

IP Security: Architecture, Authentication header, Encapsulating security payloads, combining security associations, key management. Firewalls
Transport Layer Security: Introduction to Secure Socket Layer, TLS, HTTPS
System Security: Idea of Intrusion, Intrusion detection, Intrusion Detection tools.

Recommended Books:

1. Cryptography and Network Security – William Stallings, Pearson Education
2. Network Security – Charlie Kaufman, Radia Perlman, Mike Speciner.
3. Applied Cryptography, Protocols, Algorithms, and Source Code in C, B. Schneier, Wiley

Course Outcomes:

1. *Understand the basic mathematical concepts to develop security algorithms.*
2. *Importance of integrity and signature algorithm and how such algorithms work.*
3. *Key management and distribution in WANs, importance of authentication and E-mail security*
4. *Application of security functions at different networking layers.*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	3	1	1	2	-	-	2	1	-	2	1
2	3	3	2	3	2	1	-	2	1	-	1	1
3	3	3	3	3	2	-	-	1	1	-	1	1
4	2	3	3	1	3	-	2	3	1	-	2	3

Course Title: Data Visualisation Lab									
Course Code: MCSELAA224							Examination Scheme		
Total Number of Lecture Hours: 30							External	36	
							Internal	14	
Lecture (L)	0	Practical (P)	4	Tutorial (T)	0	Total Credits			2

Course Objectives

- *To introduce students to the core principles of visual perception, Gestalt principles, and their application to effective data visualization design.*
- *To equip students with the skills necessary to design and implement diverse data visualizations, leveraging interaction techniques and visual mapping strategies.*
- *To explore emerging trends, advanced techniques, and real-time data visualization technologies in order to develop innovative visualization applications.*

List of Experiments

1. Implement basic visualizations (bar charts, line graphs) using Python (Matplotlib, Seaborn) for one- and multi-dimensional datasets.
2. Create visualizations applying Gestalt principles (proximity, similarity, continuity) and analyze their impact on data interpretation.
3. Develop interactive visualizations using filtering, zooming, and linking with tools like Tableau or Plotly for multi-dimensional data.
4. Visualize geographic data (maps, heatmaps) using tools like GeoPandas or ArcGIS to represent spatial information effectively.
5. Visualize complex data (volumetric data, vector fields) using tools like Mayavi or Paraview for scientific applications.
6. Develop a collaborative system for real-time data interaction and shared visualization views.
7. Create dynamic visualizations that update with live data (e.g., stock market) and explore performance challenges.
8. Compare visualization methods (scatter plots, heatmaps) and assess their effectiveness for different data types.

Course Learning Outcomes:

CLO1: Apply visual perception principles and Gestalt laws in designing efficient and meaningful data visualizations.

CLO2: Develop and evaluate effective interactive visualizations using different data types and interaction techniques

CLO3: Visualize complex datasets, including volumetric data, GIS data, and dynamic processes, using advanced tools and techniques.

CLO4: Understand and implement emerging trends in data visualization, including immersive technologies and real-time visualization systems.

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	2	2	3	2	1	1	-	1	1	2	0	2
2	2	3	3	2	3	2	-	2	3	3	2	3
3	3	3	3	3	3	1	-	1	3	2	2	3
4	3	3	3	2	3	2	1	1	3	2	3	3

Course Title: Big Data Analytics Lab							
Course Code: MCSELAB224						**Examination Scheme**	
Total Number of Lecture Hours: 30						**External**	**36**
						Internal	**14**
Lecture (L)	**0**	**Practical (P)**	**4**	**Tutorial (T)**	**0**	**Total Credits**	**2**

Course Objectives

1. *Hands-on experience in Hadoop ecosystem components.*
2. *Practice with Spark-based big data processing.*
3. *Build simple real-time analytics pipelines.*

List of Experiments

1. HDFS File Operations and Word Count using MapReduce
2. Data Loading using Flume and Sqoop
3. Querying Big Data using HiveQL
4. Processing large datasets with Spark Core and Spark SQL
5. Real-time data stream processing using Spark Streaming and Kafka
6. Sentiment analysis using Spark MLlib
7. Building a Recommendation Engine using collaborative filtering

This is only a suggested list of experiments/simulations. The instructor is encouraged to familiarize students with additional relevant exercises.

Course Learning Outcomes:

After successful completion of the course, the students will be able to:

CLO1: *Demonstrate HDFS and Hadoop ecosystem usage*

CLO2: *Perform batch and real-time processing using Spark*

CLO3: *Design and implement big data analytics workflows*

CLO4: *Apply machine learning algorithms using*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
1	3	3	3	2	2	-	-	-	-	-	-	3
2	2	3	3	3	3	-	-	-	-	-	-	3
3	3	3	3	3	3	1	1	-	1	1	1	3
4	3	3	3	3	3	1	-	-	1	1	1	3

Course Title: Data Warehouse and Data Mining Lab												
Course Code: MCSELAC224								Examination Scheme				
Total Number of Lecture Hours: 30								External		36		
								Internal		14		
Lecture (L)	0	Practical (P)	4	Tutorial (T)		0	Total Credits					2

Course Objectives

1. *To implement data preprocessing and transformation methods.*
2. *To practice data mining algorithms using open-source tools like Weka, Python*
3. *To evaluate and visualize mining results effectively.*

List of Experiments

1. Data Cleaning and Preprocessing using Pandas
2. Dimensionality Reduction using PCA
3. Implementation of Apriori Algorithm and FP-Growth
4. Classification using Decision Tree and Naive Bayes
5. Clustering using k-Means and DBSCAN
6. Text Classification using NLP
7. Data Visualization with Matplotlib and Seaborn
8. Association Rule Mining using Weka
9. Predictive Modeling with Logistic Regression

Note: This is only a suggested list of Experiments

Course Learning Outcomes:

After successful completion of the course, the students will be able to:

CLO1: Perform preprocessing and transformation on various datasets.

CLO2: Implement and evaluate data mining algorithms using tools.

CLO3: Analyze the performance and visualization of mining techniques.

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	-	-	-	-	-	-	-	-	-	-
2	3	3	3	3	2	-	-	-	2	-	-	2
3	2	3	3	2	-	-	-	-	-	2	-	-

Course Title: Data Security & Access Control Lab												
Course Code: MCSELAD224								Examination Scheme				
Total Number of Lecture Hours: 30								External		36		
								Internal		14		
Lecture (L)	0	Practical (P)	4	Tutorial (T)		0	Total Credits					2

List of Experiments

1) Simulate Access Control Lists (ACLs) using Python dictionaries, and compare Discretionary Access Control (DAC) with Mandatory Access Control (MAC).
2) Implement simple access control policies using Python scripts, and test them with simulated user requests.
3) Simulate Attribute-Based Access Control (ABAC) using user attributes in Python, and compare it with traditional ACL methods.
4) Analyse a real-world access control implementation (e.g., in healthcare or government) and prepare a brief report on its effectiveness.
5) Develop a basic Role-Based Access Control (RBAC) system by mapping users, roles, and permissions using Python.
6) Extend the RBAC system to include role hierarchies and permission inheritance for more efficient access management.
7) Compare the behaviour of RBAC, DAC, and MAC models through simple Python simulations and discuss their respective strengths and weaknesses.
8) Review a case study of a real-world RBAC implementation (e.g., in a banking environment) and document its key features in a report.
9) Simulate Biba's integrity model in Python.
10) Simulate the Clark-Wilson security model using Python

This is only a suggested list of experiments/simulations. The instructor is encouraged to familiarize students with additional relevant exercises.

Computing Resources

- **Operating Systems:** Windows, Linux (e.g., Ubuntu)
- **Programming Language:** Python

Virtualization Tools (Optional): VirtualBox or Docker

Course Learning Outcomes:

CLO1: Implement and simulate various access control models (DAC, MAC, RBAC, ABAC) and security models (Biba, Clark-Wilson) using Python. (Apply, Understand)
CLO2: Analyze and compare the effectiveness, strengths, and limitations of different access control mechanisms through experiments and simulations. (Analyze, Evaluate)
CLO3: Develop role-based access control systems with extensions such as role hierarchies and permission inheritance for efficient access management. (Apply, Create)
CLO4: Investigate and report on real-world access control implementations in domains such as healthcare, banking, and government, highlighting challenges and best practices. (Analyze, Evaluate, Communicate)

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	2	1	3	–	–	–	–	–	–	2
2	3	3	2	3	2	–	–	–	–	1	–	2
3	3	2	3	2	3	–	–	–	–	–	1	2
4	2	3	2	3	2	–	–	1	2	3	2	3

Course Title: Web Analytics & Development Lab							
Course Code: MCSELAE224					Examination Scheme		
Total Number of Lecture Hours: 30					External	36	
					Internal	14	
Lecture (L)	0	Practical (P)	4	Tutorial (T)	0	Total Credits	2

Course Objectives

1. *To impart practical skills for collecting, analyzing, and interpreting web data using industry-standard tools and techniques.*
2. *To enable students to implement web tracking mechanisms like cookies, session tracking, and user behavior monitoring.*
3. *To train students in using analytics platforms such as Google Analytics for deriving actionable insights from user interaction data.*
4. *To develop hands-on expertise in creating dashboards and reports for evaluating web performance and supporting data-driven decisions.*

List of Experiments

1. Create a basic responsive website using HTML, CSS, and JavaScript.
2. Implement form validation and interactivity with JavaScript.
3. Develop a simple web application using a backend framework (Node.js/PHP).
4. Connect a web application to a database and retrieve data.
5. Set up Google Analytics for a test website.
6. Track website traffic, bounce rate, and user flow.
7. Set goals, create dashboards, and interpret analytics data.
8. Perform A/B testing using Google Optimize.
9. Analyze SEO performance using Google Search Console.
10. Visualize web traffic using heatmap tools (e.g., Hotjar/Clarity).

This is only a suggested list of experiments/simulations. The instructor is encouraged to familiarize students with additional relevant exercises.

Course Learning Outcomes:

1. *Develop and deploy dynamic and responsive web applications.*
2. *Integrate Google Analytics and other tools for web tracking.*
3. *Analyze web traffic data and interpret reports.*
4. *Perform testing and optimization for improving website performance.*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	3	2	2	3	1	-	-	-	1	-	2
2	2	3	2	3	3	-	-	-	-	2	-	2
3	2	3	3	3	2	1	-	1	-	2	1	2
4	2	2	3	3	3	-	1	-	-	3	-	2

Course Title: Knowledge Discovery Lab							
Course Code: MCSELAF224					Examination Scheme		
Total Number of Lecture Hours: 30					External	36	
					Internal	14	
Lecture (L)	0	Practical (P)	4	Tutorial (T)	0	Total Credits	2

Course Objectives

1. *To practice data preprocessing techniques on real-world datasets.*
2. *To implement and evaluate classification and clustering algorithms.*
3. *To apply association rule mining on transactional datasets.*
4. *To develop and present a complete knowledge discovery pipeline.*

List of Experiments

1. Data cleaning and preprocessing using Python or R.
2. Implementation of classification algorithms (e.g., Decision Tree, Naive Bayes).
3. Implementation of clustering algorithms (e.g., K-Means, DBSCAN).
4. Association rule mining using Apriori and FP-Growth.
5. Web and text mining using open-source tools.
6. Mini project: Apply data mining pipeline on a real-world dataset.

This is only a suggested list of experiments/simulations. The instructor is encouraged to familiarize students with additional relevant exercises.

Course Learning Outcomes:

1. *Perform pre-processing and feature selection techniques on datasets.*
2. *Build and evaluate machine learning models for classification and clustering.*
3. *Implement and interpret association rules.*
4. *Design a mini-project involving end-to-end data mining.*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	3	2	2	2	-	-	-	-	-	-	-
2	3	2	3	2	2	-	-	-	-	-	-	-
3	2	2	2	2	2	-	-	-	-	-	-	-
4	3	3	3	3	3	2	-	-	2	1	-	2

Course Title: Introduction to Deep Learning Lab									
Course Code: MCSELAG224						Examination Scheme			
Total Number of Lecture Hours: 30						External	36		
						Internal	14		
Lecture (L)	0	Practical (P)	4	Tutorial (T)	0	Total Credits	2		

Course Objectives

To enable students with both theoretical understanding and practical implementation skills in modern neural network architectures, building a single-layer perceptron from scratch for binary classification, and implementing a basic Artificial Neural Network (ANN) using TensorFlow and Keras for tasks like handwritten digit recognition with the MNIST dataset.

List of Experiments

1. Design a single unit perceptron for classification of a linearly separable binary dataset without using pre-defined models.
2. Design and implement a basic Artificial Neural Network (ANN) using TensorFlow & Keras for a simple classification task (e.g., handwritten digit recognition using MNIST dataset).
3. Build an Artificial Neural Network by implementing the Backpropagation algorithm and test the same using appropriate data sets.
4. Design and implement an Image classification model to classify a dataset of images using Deep Feed Forward NN. Record the accuracy corresponding to the number of epochs. Use the MNIST datasets.
5. Design and implement a CNN model to classify multi category image datasets. Record the accuracy corresponding to the number of epochs. Use the MNIST, CIFAR-10 datasets.
6. Use the concept of Data Augmentation to increase the data size from a single image.
7. Implement the standard VGG-16 & 19 CNN architecture model to classify multi category image dataset and check the accuracy.
8. Implement RNN for sentiment analysis on movie reviews
9. Implement Bi-directional LSTM for sentiment analysis on movie reviews.
10. Implement Auto encoders for image denoising on MNIST dataset.

This is only a suggested list of experiments/simulations. The instructor is encouraged to familiarize students with additional relevant exercises.

Course Learning Outcomes:

1. *Understand and implement the fundamentals of neural networks and perceptron-based models for solving linearly separable classification problems.*
2. *Design, develop, and evaluate deep neural network architectures including feedforward networks and convolutional neural networks for image classification tasks.*
3. *Apply advanced deep learning models such as RNN and Bi-LSTM for natural language processing tasks like sentiment analysis.*
4. *Demonstrate the application of autoencoders for unsupervised learning tasks such as image denoising and feature extraction.*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	2	2	2	-	-	1	1	1	-	2
2	3	3	3	2	3	1	-	1	2	2	1	2
3	3	3	3	3	3	1	-	1	2	2	1	3
4	3	2	3	3	3	1	-	1	2	2	1	2

Course Title: Pattern Recognition Lab							
Course Code: MCSELAH224					Examination Scheme		
Total Number of Lecture Hours: 30					External	36	
					Internal	14	
Lecture (L)	0	Practical (P)	4	Tutorial (T)	0	Total Credits	2

Course Objectives

- *To practically implement pattern recognition algorithms and methods.*
- *To build classifiers and clustering models based on different approaches (Bayesian, nonparametric, machine learning models).*
- *To analyze and interpret results obtained from various pattern recognition methods.*
- *To develop skills for applying pattern recognition techniques on real-world datasets*

List of Experiments

1. Implement and visualize basic probability distributions (e.g., Gaussian, Binomial) and random processes.
2. Implement Bayes Classifier for two-class classification using Gaussian assumption.
3. Estimate parameters (mean, variance) from data using Maximum Likelihood Estimation (MLE) and Bayesian Estimation.
4. Develop a K-Means Clustering algorithm from scratch and compare it with scikit-learn's KMeans.
5. Train and test a simple Hidden Markov Model (HMM) using discrete observations (e.g., Weather prediction).
6. Build a K-Nearest Neighbour (KNN) Classifier from scratch and validate it on a real dataset (e.g., Iris Dataset).
7. Apply Principal Component Analysis (PCA) for dimensionality reduction and visualize 2D projections.
8. Implement Linear Discriminant Analysis (LDA) for classification tasks.
9. Build and evaluate a Support Vector Machine (SVM) classifier using a sample dataset.

This is only a suggested list of experiments/simulations. The instructor is encouraged to familiarize students with additional relevant exercises.

Course Learning Outcomes:

1. *Understand and implement fundamental statistical models for pattern recognition.*
2. *Design and evaluate supervised learning models using Bayesian and nonparametric methods.*
3. *Implement clustering algorithms and validate unsupervised learning models.*
4. *Apply dimensionality reduction techniques and construct interpretable models*
5. *Use advanced classifiers like SVMs, Decision Trees, and HMMs to solve practical problems.*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	3	3	2	3	2	1	1	1	1	1	2
2	3	3	3	2	3	2	1	1	1	1	1	2
3	3	3	3	3	3	2	1	1	1	1	1	2
4	3	3	3	3	3	2	1	1	1	1	1	3
5	3	3	3	3	3	2	2	1	1	1	1	3

Course Title: Intrusion Detection Lab							
Course Code: MCSELAI224					Examination Scheme		
Total Number of Lecture Hours: 50					External	36	
					Internal	14	
Lecture (L)	0	Practical (P)	4	Tutorial (T)	0	Total Credits	2

List of Experiments

1. **Study and Demonstration of Common Network Threats**
   - Simulate basic network attacks such as port scanning, SYN flood, and packet sniffing using tools like Nmap, Hping3, and Wireshark.
2. **Firewall Configuration and Testing**
   - Configure a host-based or network firewall (e.g., iptables or pfSense) and test its effectiveness against various attack vectors.
3. **Virtual Private Network (VPN) Setup and Security Testing**
   - Create a VPN using OpenVPN or WireGuard and analyze the security of data transmission over public networks.
4. **Installation and Basic Configuration of Snort IDS**
   - Set up Snort on a Linux system and capture normal and malicious network traffic.
5. **Writing Custom Snort Rules**
   - Create and test custom Snort rules to detect specific attacks such as ICMP floods, port scans, or login attempts.
6. **Detection of Application Layer Attacks**
   - Simulate attacks like SQL Injection, Cross-Site Scripting (XSS), and buffer overflows and analyze detection using Snort or other IDS tools.
7. **Log Analysis and Intrusion Detection using SIEM Tools**
   - Use tools like Splunk or ELK Stack to analyze logs from hosts and detect anomalies or intrusions.
8. **Performance Evaluation of an IDS System**
   - Compare detection accuracy, false positives/negatives, and resource usage under different Snort rule sets or other IDS configurations.
9. **Simulation of Malware Behavior (Viruses, Worms) in a Controlled Environment**
   - Use tools like Cuckoo Sandbox to observe malware behavior and examine detection by IDS.
10. **Case Study: Cost-Sensitive Intrusion Detection**

This is only a suggested list of experiments/simulations. The instructor is encouraged to familiarize students with additional relevant exercises.