ST JOSEPH'S UNIVERSITY

BENGALURU-27

ST. JOSEPH'S UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE

SYLLABUS FOR POSTGRADUATE PROGRAMME

M.Sc. (Cyber Security & Artificial Intelligence)

Program Outcomes of the M.Sc CS & AI Programme are:

PO1	**Advanced Computing Knowledge** Apply advanced knowledge of computer science, artificial intelligence, machine learning, data science, and cybersecurity principles to solve complex computing problems.
PO2	**Cybersecurity Expertise** Design, implement, and evaluate secure systems, networks, applications, and infrastructure using appropriate cybersecurity principles, tools, and techniques.
PO3	**Artificial Intelligence and Intelligent Systems** Develop and apply AI and machine learning models to analyse data, automate decision-making, and address real-world problems while considering performance, reliability, and security.
PO4	**Problem Analysis and Solution Design** Identify, formulate, analyse, and solve complex computing and cybersecurity problems using logical reasoning, computational thinking, algorithms, and appropriate technological approaches.
PO5	**Research and Innovation** Conduct independent research, critically evaluate existing approaches, and develop innovative solutions in emerging areas of cybersecurity and artificial intelligence.
PO6	**Ethical, Legal, and Responsible Practice** Apply ethical principles, professional standards, privacy regulations, and legal frameworks in the responsible development and deployment of AI and cybersecurity solutions.
PO7	**Communication, Collaboration, and Lifelong Learning** Communicate technical ideas effectively, work collaboratively in multidisciplinary teams, demonstrate leadership and professional skills, and continuously adapt to emerging technologies in cybersecurity and artificial intelligence.

SEMESTER 1

Code Number	Title	No of Hours of teaching per week	No of credits	Continuous Internal Assessment (CIA) Marks	End Semester Marks	Total marks
THEORY						
CSAI7126	Applied Mathematics for Cyber Security and Artificial Intelligence	04	04	50	50	100
CSAI7226	Design and Analysis of Algorithms	04	04	50	50	100
CSAI7326	Computer Networks and Information Security	04	04	50	50	100
CSAI7426	Cyber Law , Ethics and Criminology	04	04	50	50	100
CSAI7526	Advanced Python Programming for AI	04	04	50	50	100
PRACTICALS						
CSAI7P126	Design and Analysis of algorithm and Information Security Lab	04	02	25	25	50
CSAI7P226	Python programming Lab	04	02	25	25	50
Total Number of credits: 24						

SEMESTER 2

Code Number	Title	No of Hours of teaching per week	No of credits	Continuous Internal Assessment (CIA) Marks	End Semester Marks	Total marks
THEORY						
CSAI8126	Advanced Operating System concepts with Linux	04	04	50	50	100
CSAI8226	Cryptography Techniques	04	04	50	50	100
CSAI8326	Cloud Security	04	04	50	50	100
CSAI8426	Machine Learning Essentials	04	04	50	50	100
CSAI8526	Big Data Analytics	04	04	50	50	100
PRACTICALS						
CSAI8P126	Cryptography Techniques Lab	04	02	25	25	50
CSAI8P226	Machine Learning Techniques Lab	04	02	25	25	50
Total Number of credits: 24						

SEMESTER 3

Code Number	Title	No of Hours of teaching per week	No of credits	Continuous Internal Assessment (CIA)Marks	End Semester Marks	Total marks
THEORY						
CSAI9126	Ethical Hacking and Penetration Testing	04	04	50	50	100
CSAI9226	Digital Forensics	04	04	50	50	100
CSAI9326	Natural Language Processing	04	04	50	50	100
CSAI9426	Deep Learning and Neural Networks with Quantum Computing	04	04	50	50	100
DEPARTMENT ELECTIVE						
CSAIDE9526	Artificial Intelligence for Cybersecurity	04	04	50	50	100
CSAIDE9626	DevOps in AI	04	04	50	50	100
PRACTICALS						
CSAI9P126	Natural Language Processing Lab	04	02	25	25	50

CSAI9P226	**Digital Forensics Lab**	**04**	**02**	**25**	**25**	**50**
CSAIRM9726	**Research Paper Presentation**	**02**	**02**	**25**	**25**	**50**
Total Number of credits: 26						

SEMESTER 4

DEPARTMENT OF COMPUTER SCIENCE AND COMPUTER APPLICATIONS(PG) (2025-2026)							
Semester 4	**Code Number**	**Title**	**No of Hours of teaching per week**	**No of credits**	**Continuous Internal Assessment (CIA)Marks**	**End Semester Marks**	**Total marks**
Project	**CSAIINT0P126**	**Industry Internship / Project Work**	32	16	200	200	400
Certification Course	**CSAI0P226**	**Online/ Certification Course**	3	3	50	50	100
Total Number of credits: 19							

KEY WORDS: DE – Departmental Elective and OE – Open Elective

CORE COURSES (CC)	
Course Title	**Code Number**
Applied Mathematics for Cyber Security and Artificial Intelligence	CSAI7126
Design and Analysis of Algorithms	CSAI7226
Computer Networks and Information Security	CSAI7326
Cyber Law , Ethics and Criminology	CSAI7426
Advanced Python Programming for AI	CSAI7526
Advanced Operating System concepts with Linux	CSAI8126
Cryptography Techniques	CSAI8226
Cloud Security	CSAI8326
Machine Learning Essentials	CSAI8426
Big Data Analytics	CSAI8526
Ethical Hacking and Penetration Testing	CSAI9126
Digital Forensics	CSAI9226
Natural Language Processing	CSAI9326
Deep Learning and Neural Networks with Quantum Computing	CSAI9426

DISCIPLINE SPECIFIC ELECTIVE COURSES (DSE)	
Course Title	**Code Number**
Artificial Intelligence for Cybersecurity	CSAIDE9526
DevOps in AI	CSAIDE9626

SKILL ENHANCEMENT COURSE (SEC)	
Course Title	**Code Number**
Design and Analysis of algorithm and Information Security Lab	CSAI7P126
Python programming Lab	CSAI7P226
Cryptography Techniques Lab	CSAI8P126
Machine Learning Techniques Lab	CSAI8P226
Natural Language Processing Lab	CSAI9P126
Digital Forensics Lab	CSAI9P226
Research Paper Presentation	CSAIRM9726
Industry Internship / Project Work	CSAIINT0P126
Online/ Certification Course	CSAI0P226

SYLLABUS

SEMESTER-I

Course Code: CSAI7126	Course Title: **Applied Mathematics for Cyber Security and Artificial Intelligence**
Course Credits: 04	Hours/Week: 04
Total Contact Hours: 52	Formative Assessment Marks: 50
Exam Marks: 50	Exam Duration: 2 Hrs

Course Outcomes (COs):
After completing the course, students will be able to:

1. Apply advanced mathematical logic to model and analyze secure systems.
2. Use linear algebra techniques in AI and cryptographic applications.
3. Apply probability and statistical methods to cyber threat analysis.
4. Perform statistical inference and data analytics for intelligent systems.
5. Formulate and solve optimization problems in AI-driven cyber security.

Unit	Title	No. of hours
I	**Advanced Mathematical Logic and Discrete Structures** Propositional and Predicate Logic: Syntax and semantics, Quantifiers and inference rules, Proof techniques: Direct, indirect, contradiction, and induction, Boolean Algebra : Boolean functions, Karnaugh maps, Boolean minimisation techniques and Lattices and Boolean lattices, Discrete	12

	structures: Relations and closures and Equivalence relations and partial orders, Recurrence relations and solving techniques.	
II	**Linear Algebra and Matrix Computations** Vector spaces and subspaces, Linear transformations and matrix representation, Rank, nullity, and dimension, Eigenvalues, eigenvectors, diagonalization, Quadratic forms and matrix factorization : LU, QR, and Singular Value Decomposition (SVD).	12
III	**Advanced Probability Theory and Stochastic Models** Axiomatic probability theory, Random variables (discrete and continuous), Joint distributions and marginal distributions, Conditional expectation and variance, Bayes' theorem and Bayesian inference, Stochastic processes: Markov chains and Poisson processes, Entropy and information measures.	12
IV	**Statistical Methods and Data Analytics** Sampling techniques and experimental design, Estimation theory: Point and interval estimation and Maximum likelihood estimation, Hypothesis testing: Parametric and non-parametric tests, Multivariate statistical analysis: Principal Component Analysis (PCA) and Cluster analysis, Regression analysis: Linear and logistic regression	12
V	**Optimization, Graph Theory and Mathematical Foundations of Machine Learning** Graph theory: Directed and undirected graphs and Connectivity, trees, shortest path algorithms, Combinatorial optimization, Linear and non-linear programming, Convex optimization techniques, Mathematical foundations of machine learning: Loss functions and Gradient descent and optimization methods, Game theory fundamentals	12

Text Books

1. **Rosen, Kenneth H.** *Discrete Mathematics and Its Applications*,8th Edition, McGraw-Hill Education, New York, 2019.
2. **Strang, Gilber,** *Linear Algebra and Its Applications*,5th Edition, Cengage Learning, Boston, 2016.
3. **Ross, Sheldon M,** *A First Course in Probability*,10th Edition, Pearson Education, New Delhi, 2019.

Reference Books

1. **Devore, Jay L,** *Probability and Statistics for Engineering and the Sciences*, 9th Edition, Cengage Learning, Boston, 2016.
2. **Bishop, Christopher M,** *Pattern Recognition and Machine Learning*, 1st Edition, Springer-Verlag, New York, 2006.
   Cover, Thomas M. and Thomas, Joy A, *Elements of Information Theory*, 2nd Edition, Wiley-Interscience, Hoboken, New Jersey, 2006.
3. **Goodfellow, Ian; Bengio, Yoshua; Courville, Aaron**, *Deep Learning*
   1st Edition, MIT Press, Cambridge, Massachusetts, 2016.
4. **Stallings, William**
   Cryptography and Network Security: Principles and Practice, 8th Edition, Pearson Education, New Delhi, 2020.
5. **Boyd, Stephen and Vandenberghe, Lieven**, *Convex Optimization*, 1st Edition, Cambridge University Press, Cambridge, 2004.
6. **West, Douglas B,** *Introduction to Graph Theory*,2nd Edition, Prentice Hall, Upper Saddle River, New Jersey, 2001.

Course Code: CSAI7226	Course Title: **Design and Analysis of Algorithms**
Course Credits: 04	Hours/Week: 04
Total Contact Hours: 52	Formative Assessment Marks: 50
Exam Marks: 50	Exam Duration: 2 Hrs

Course Outcomes:

1. Design and implement efficient algorithms using appropriate paradigms to solve cybersecurity and AI-related problems.
2. Analyze and compare algorithms based on time and space complexity for secure and large-scale systems.
3. Apply graph, greedy, dynamic programming, and heuristic algorithms to security applications such as secure routing, attack graphs, and intelligent threat analysis.
4. Select and justify suitable algorithms by considering performance, scalability, and security requirements in AI-driven cybersecurity systems.
5. To enable students to critically evaluate and optimize algorithms for secure, scalable, and intelligent systems in cybersecurity and AI.

Unit- wise Syllabus

Unit	Title	No. of hours
I	**INTRODUCTION:** **Introduction**: Notion of Algorithm, Fundamentals of Algorithmic Problem Solving, Fundamentals of the Analysis of Algorithmic Efficiency: Analysis Framework, Time and space complexity, Asymptotic Notations and Basic Efficiency Classes, Algorithm design paradigms. **Brute Force**: Selection Sort and Bubble Sort.	12

II	**DIVIDE AND CONQUER AND GREEDY METHOD:** **Divide and Conquer**: Merge sort, Quicksort, Multiplication of Long Integers, Strassen's Matrix Multiplication. **Greedy Method:** Minimal Spanning Tree (Prims and Kruskal's Algorithm), Single source Shortest Paths Problem: Dijkstra's algorithm and Bellman-Ford , Fractional Knapsack Problem.	12
III	**SEARCH, HEURISTICS, AND ADVERSARIAL ALGORITHMS** **Uninformed search**: BFS, DFS, Iterative Deepening, **Informed search:** Greedy Best-First Search, A*, Heuristic design: admissibility and consistency, Game-tree search: Minimax, Alpha–Beta pruning.	10
IV	**DYNAMIC PROGRAMMING AND GRAPH THEORY** **Dynamic programming:** Computing a Binomial Coefficient, Warshall's and Floyd's Algorithms, 0/1 Knapsack Problem and Memory Functions. All pair Shortest path algorithms, **Graph theory:** Graph representations in AI and cybersecurity, Connectivity and ordering: Connected and strongly connected components, Topological sorting (DAGs), Flow networks: Maximum flow problem, Ford–Fulkerson method (overview), Maximum flow and minimum cut. Attack graphs and trust graphs	14
V	**ADVANCED ALGORITHM DESIGN AND TECHN IQUES** **Backtracking**: N-Queen's Problem, Sum of Subset Problem. **Branch-and-Bound**: Travelling Salesperson Problem, Assignment Problem **Decision Trees**: Decision Trees for Sorting **NP and NP-Complete Problems**: Basic Concepts, Non- Deterministic Algorithms, P, NP, NP Complete, and NP-Hard classes.	12

TEXT BOOKS

- Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2022). Introduction to algorithms (4th ed.). MIT Press.
- E. Horowitz and S. Sahani, Fundamentals of Computer Algorithms, Galgotia, New Delhi.

REFERENCES

- Aho, J. Hopcroft and J.Ullman, The Design and Analysis of Computer Algorithms, Addison Wesley.
- S.E.Goodman and S.T.Hedetniemi, Introduction to the Design and Analysis of Algorithms, McGraw Hill.
- G.Brassard, and P.Bratley, Algorithmics, PHI.
- S.K.Basu, Design Methods and Analysis of Algorithms, PHI.

Course Code: CSAI7326	Course Title: **COMPUTER NETWORKS AND SECURITY**
Course Credits: 04	Hours/Week: 04
Total Contact Hours: 52	Formative Assessment Marks: 50
Exam Marks: 50	Exam Duration: 2 Hrs

Course Outcomes

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

- **CO1:** Demonstrate knowledge of networking concepts and network security fundamentals.
- **CO2:** Identify and analyze security attacks and vulnerabilities in computer networks.
- **CO3:** Explain and apply cryptographic algorithms and protocols used in secure communication systems.

Unit- wise Syllabus

Unit	Topics	No. of hours
I	**Introduction to Computer Networks** Introduction to computer networks, types of networks, network components, topologies, network models, data transmission techniques, wireless networking, basics of network security, subnetting, and emerging networking trends. Routers, switches, hubs, firewalls, load balancers, proxy servers, network interface cards (NICs), wireless access points, modems, network attached storage (NAS), VPN concentrators, and content delivery networks (CDNs).	**12**
II	**Network Protocols** OSI Vs TCP/IP protocol suite, Ethernet,IEEE standards, Routing protocols:OSPF,Distance vector routing,ARP, DNS, DHCP, HTTP, FTP, SMTP, SNMP, ICMP, IPv4 and IPv6, BGP, TLS/SSL, and NTP.	**12**
III	**Introduction to Cryptography:** Security Architecture,Three aspects of security,CIA triad,security attacks, Model for security,classical encryption methods,stream ciphers :CeaserAffine polyalphabetic ciphers: Vignere , Hill ciphers.Block ciphers: Fiestel, DES,AES, block cipher modes, key distribution techniques, random number generation, hash functions, and asymmetric encryption. **Firewalls and Intrusion Detection/Prevention:** Introduction to firewalls, packet filtering firewalls, stateful inspection firewalls, intrusion	**12**

	detection systems (IDS), intrusion prevention systems (IPS), security policies, and rule configuration.	
IV	**Wireless Network Security** Introduction to wireless security, wireless threats and vulnerabilities, Wi-Fi security standards, WEP, WPA, WPA2, WPA3, Wi-Fi Protected Setup (WPS), enterprise wireless security, and wireless security best practices.	**12**
V	**Secure Network Infra structure management** Secure configuration management, access control and authentication, network segmentation and zoning, patch management, network device hardening, encryption and data protection, endpoint security, and security policies and procedures.	**12**

Text Books

1. William Stallings, *Cryptography and Network Security: Principles and Practice*, Pearson Education, 2017.
2. Andrew S. Tanenbaum and David J. Wetherall, *Computer Networks*, Pearson Education, 2022.

Reference Books

1. Charlie Kaufman, Radia Perlman, Mike Speciner, *Network Security: Private Communication in a Public World*, O'Reilly Media, 2011.
2. James F. Kurose and Keith W. Ross, *Computer Networking: A Top-Down Approach*, 7th Edition, Pearson, 2017.
3. Christof Paar and Jan Pelzl, *Understanding Cryptography*, Springer, 2010.

Course Code: CSAI7426	Course Title: **Cyber Law, Ethics and Criminology**
Course Credits: 04	Hours/Week: 04
Total Contact Hours: 52	Formative Assessment Marks: 50
Exam Marks: 50	Exam Duration: 2 Hrs

Course Outcomes

After successful completion of this course, students will be able to

CO1: Explain the legal framework governing cyberspace, including the IT Act, digital contracts, and jurisdictional issues.

CO2: Identify, classify, and analyze various types of cyber-crimes using criminological theories.

CO3: Examine ethical issues related to cyber space, data privacy, intellectual property, and Artificial Intelligence.

CO4: Apply legal procedures and forensic principles for handling digital evidence and cyber-crime investigations.

CO5: Evaluate global cyber laws, data protection regulations, and emerging legal challenges in AI and cloud computing.

Unit- wise Syllabus

Unit	Topics	No. of hours
I	**Foundations of Cyber Law** Introduction to Cyber Law and Legal Framework, Evolution of Cyber Space and Cyber Jurisprudence, Information Technology Act, 2000 – Objectives and Scope, Amendments to IT Act (2008), Digital Signatures, Electronic Governance, Certifying Authorities, Cyber	**12**

	Contracts and E-Commerce Legal Issues, Jurisdiction issues in Cyberspace, Role of Cyber Law in AI-driven Systems.	
II	**Cyber Crimes and Digital Criminology** Introduction to Cyber Criminology, Classification of Cyber Crimes: Crimes against Individuals, Crimes against Property, Crimes against Organizations and Crimes against Government, Cyber Stalking, Cyber Defamation, Identity Theft, Cyber Obscenity and Pornography, Financial Frauds and Cryptocurrency Crimes, Cyber Crime and Cyber Terrorism, Criminological Theories applied to Cyber Crime, Role of AI in Predicting and Preventing Cyber Crimes.	**12**
III	**Cyber Ethics and Professional Responsibility** Ethics in Cyberspace, Ethical Theories and Models, Privacy, Surveillance, and Data Protection Ethics, Ethical Issues in Artificial Intelligence: Bias in AI, Explainable AI and Responsible AI, Intellectual Property Rights (IPR), Software Piracy and Plagiarism, Codes of Ethics (ACM, IEEE, ISC^2).	**12**
IV	**Digital Evidence, Forensics and Legal Procedures** Digital Evidence: Types and Characteristics, Legal Admissibility of Digital Evidence, Chain of Custody, Cyber Forensics Process Model, Role of Expert Witness, Investigation Procedures under IT Act, AI Tools in Digital Forensics, Case Studies on Cyber Crime	**12**

	Investigations. Phishing Email Scam Investigation, Online Banking Fraud Case and Social Media Account Hacking Case.	
V	**Global Cyber Laws, Data Protection and Emerging Issues (12 Hours)** International Cyber Laws and Treaties, GDPR Regulations, Indian Data Protection Laws (DPDP Act, 2023), Cyber Warfare and National Security, Legal Challenges in Cloud Computing and AI, Ethical and Legal Issues in Autonomous Systems, Future Trends in Cyber Law and AI Governance.	**12**

Text Books

1. Pavan Duggal, *Cyber Law in India*, 2nd Edition, Saakshar Law Publications, New Delhi, 2014.
2. Talwant Singh, *Cyber Law & Information Technology*, Revised Edition, Tata McGraw-Hill Education, New Delhi, 2016.
3. David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*, 2nd Edition, Polity Press, Cambridge, 2018.

Reference Books

1. Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3rd Edition, Academic Press (Elsevier), London, 2011.
2. Orin S. Kerr, *Computer Crime Law*, 4th Edition, West Academic Publishing, St. Paul, Minnesota, 2018.
3. Luciano Floridi, *The Ethics of Information*, 1st Edition, Oxford University Press, Oxford, 2013.

4. Luciano Floridi (Editor), *The Oxford Handbook of Information and Computer Ethics* 1st Edition, Oxford University Press, Oxford, 2010.

5. Ian Goodfellow, Yoshua Bengio, Aaron Courville, *Deep Learning*,1st Edition, MIT Press, Cambridge, Massachusetts, 2016.

6. William Stallings, *Cryptography and Network Security: Principles and Practice* 8th Edition, Pearson Education, New Delhi, 2020.

7. Chris Reed & John Angel (Editors), *Computer Law: The Law and Regulation of Information Technology*, 7th Edition, Oxford University Press, Oxford, 2018.

8. Paul Craig & Gráinne de Búrca, *EU Law: Text, Cases, and Materials*, 6th Edition, Oxford University Press, Oxford, 2015.

Course code :CSAI7526	Course Title: **Advanced Python Programming for AI**
Course Credits: 04	Hours/Week: 04
Total Contact Hours: 60	Formative Assessment Marks: 50
Exam Marks: 50	Exam Duration: 02Hrs

Course Outcomes (COs):

At the end of this course, the student will be able to:

CO1	Acquire a comprehensive understanding of fundamental Python concepts and syntax.
CO2	Develop an understanding of advanced Python concepts and techniques, including object-oriented programming, functional programming, and module/package management.
CO3	Apply Python programming skills to develop practical solutions to real-world problems, including data manipulation, web scraping, GUI development, API integration, and database management.

CO4	Analyse and evaluate different approaches and techniques in Python programming to select the most appropriate solution for a given problem.
CO5	Synthesize knowledge and skills acquired throughout the course to design and implement complex software projects, demonstrating creativity and innovation.
CO6	Create fully functional Python applications and projects that showcase proficiency in various Python libraries, frameworks, and tools, meeting the requirements of diverse stakeholders and industries.

Unit- wise Syllabus

UNIT	TOPIC	Hours
I	**Python Fundamentals** **Introduction to Python**: Overview of Python programming language Installing Python and setting up development environment Basic syntax, variables, Strings and data types, Conditional statements, Loops, Loops manipulation **Data Structures and Functions:** List, Dictionary, Tuple, Set, Functions, and Parameter Passing Error Handling with try-except. **Object Oriented Programming** : Concept of class, object and instance, inheritance **Packages**: modules, importing own module as well as external modules, Understanding Packages	**12**
II	**Data Manipulation with NumPy , Pandas and Plotting with Matplotlib** **Introduction to NumPy:** Arrays, Basic array operations and slicing Introduction to Pandas data structures, Series and Data Frame, Data ingestion, manipulation, and cleaning with Pandas. **Introduction to Data Visualization:** Importance of data visualization, Introduction to Matplotlib for plotting Basic plotting: line plots, scatter plots, bar plots Customizing plots with labels, titles, and legends.	**12**

III	**Graphical User Interface (GUI) Development** Introduction to GUI Programming, GUI Development with Tkinter, Handling Events and User Input **Widget** : Advanced Widget Customization (Tkinter Wrappers: CustomTkinter, ttkbootstrap, Tkinter Canvas), Data Visualization in GUI Applications, Building Interactive Applications, GUI Integration with Data Manipulation, Deployment, and Distribution.	**12**
IV	**Web Scraping and API** **Web Scraping** Introduction to Web Scraping Overview of Web Scraping, HTML Fundamentals, Inspecting Web Pages, Web Scraping with Beautiful Soup, Scraping Multiple Pages and Pagination, Handling Forms and Logins, Handling Dynamic Content. **APIs** Introduction to APIs, Understanding APIs, API Documentation, Authentication and Authorization, Making API Requests and API Data Manipulation.	**12**
V	**Introduction to MongoDB and Project Work** Overview of MongoDB, Introduction to PyMongo, Installation and Setup, Basic CRUD Operations, Data Modelling and Schema Design, Data Replication and Sharding, Transactions and Consistency. **Project Work and Applications**	**12**

REFERENCES:

1. "Fluent Python: Clear, Concise, and Effective Programming", Second Edition (Grayscale Indian Edition) Paperback – 6 May 2022

2. "Python in a Nutshell Paperback" by Alex Martelli , Anna Ravenscroft, Steve Holden – 4 May 2017

3. "Python Crash Course" by Eric Matthes, 2nd Edition, published by No Starch Press in 2019.

4. "Automate the Boring Stuff with Python" by Al Sweigart, 2nd Edition, published by No Starch Press in 2019.

5. "Effective Python: 90 Specific Ways to Write Better Python" by Brett Slatkin, 2nd Edition, published by Addison-Wesley Professional in 2020.

6. Python Distilled (Developer's Library) 1st Edition-22 September 2021

Course Code : CSAI7P126	Course Title: **Design and Analysis of Algorithms and Information Security Lab**
Course Credits: 1.5	Hours/Week: 03
Total Contact Hours: 36	Formative Assessment Marks: 25
Exam Marks: 25	Exam Duration: 02Hrs

PART A: **Design and Analysis of algorithms Lab Programs**

1. Program to implement Linear Search and Binary Search for detecting suspicious IP addresses in network security logs and analyze their execution time.
2. Program to implement Quick Sort for sorting large-scale network traffic or AI training data and compare their performance.
3. Program to implement Merge Sort for stable and efficient organization of encrypted data blocks in secure storage systems.
4. Program to implement Activity Selection using a Greedy approach for efficient scheduling of intrusion detection processes.
5. Program to implement Dijkstra's algorithm to determine the shortest and most secure routing path in a communication network.
6. Program to implement Prim's algorithm to design a minimum-cost secure network infrastructure.
7. Program to implement the 0/1 Knapsack algorithm using Dynamic Programming for optimal allocation of encrypted files in limited secure storage.
8. Program to find the Longest Common Subsequence (LCS) between malware signatures to measure similarity and detect variants.
9. Program to solve the N-Queens problem using Backtracking and relate it to access-control constraint satisfaction.
10. Program to experimentally analyze and compare the time complexity of two algorithms commonly used in AI data preprocessing.

PART B: **Information Security Lab Programs**

1. Execution of basic network commands and network configuration

2. Write a socket program for the implementation of echo.

3. Using TCP/IP sockets, write a client – server program to make the client send the file name and to make the server send back the contents of the

4. Write a program on a datagram socket for client/server to display the messages on client side, typed at the server side.

5. Write a program to implement the Token Passing algorithm.

6. To configure WPA2/WPA3 and analyze authentication using Wi-Fi Router, Wireshark

7. Write a program to encrypt and decrypt a Password.

8. Implement the substitution mono alphabetic technique by using the Caesar Cipher algorithm.

9. To configure a firewall with IDS/IPS rules to monitor, detect, and block unauthorized network access

10. To implement the Data Encryption Standard (DES) algorithm to encrypt and decrypt a given plaintext using a secret key.

11. To develop an application that secures digital information through AES-based encryption and decryption

Course Code : CSAI7P226	Course Title: **Python Programming lab**
Course Credits: 1.5	Hours/Week: 03
Total Contact Hours: 36	Formative Assessment Marks: 25
Exam Marks: 25	Exam Duration: 02Hrs

Program List

1. Python Basics:
2. Write a program to calculate the factorial of a number using a recursive function.
3. Implement a program to find the sum of all elements in a given list.
4. Create a program to count the occurrences of each word in a text file.

5. Data Manipulation with Pandas and NumPy :

a) Load a dataset using Pandas and display basic information such as the number of rows, columns, and data types.
b) Perform data cleaning tasks like handling missing values and removing duplicates in a dataset.
c) Use NumPy to create arrays and perform basic operations such as element-wise addition, subtraction, multiplication, and division.

6. Plotting with Matplotlib:

a) Create a line plot to visualize the trend of a time-series dataset.
b) Generate a scatter plot to analyze the relationship between two variables in a dataset.
c) Plot multiple data sets on the same figure with customized colors, markers, and labels.

7. Object-Oriented Programming:

a) Implement a class representing a bank account with methods to deposit, withdraw, and check balance.

b) Create a class hierarchy representing different shapes (e.g., circle, rectangle, triangle) with methods to calculate area and perimeter.

8. Web Scraping:

a) Write a Python program to scrape a website of your choice and extract specific information. The program should:

- Use BeautifulSoup library for parsing HTML.
- Extract data such as headlines, links, or any relevant information from the webpage.
- Display the extracted information in a structured format.

9. GUI (Graphical User Interface):

a) Design a Python GUI application using Tkinter that calculates the area of a circle. The program should accept user input for the radius, and when the user clicks a button, it should display the calculated area.

b) Develop a GUI-based to-do list application using Tkinter. The application should allow users to add tasks, mark tasks as completed, and delete tasks from the list.

c) Create a simple calculator using Tkinter that performs basic arithmetic operations (addition, subtraction, multiplication, division). The calculator should have buttons for each operation and a display area to show the result of calculations.

10. Web Scraping:

a) Write a Python script to scrape a news website and extract the headlines and summaries of the latest articles. Display this information in the console.

b) Develop a web scraper to extract product information (such as name, price, and description) from an e-commerce website. Save this information to a CSV file.

c) Create a Python program to scrape a weather website and extract the current temperature, humidity, and weather conditions for a specific location. Display this information in a user-friendly format.

11. API (Application Programming Interface):

a) Develop a Python script that interacts with the OpenWeatherMap API to retrieve the current weather conditions for a given city. Display the temperature, weather description, and other relevant data.

b) Write a program to access the Twitter API and fetch recent tweets based on a specific hashtag. Display the usernames and tweet content.

12. MongoDB:

a) Write a Python script that connects to a MongoDB database and inserts a new document into a collection. Include fields such as name, age, and email address.

b) Develop a program to query a MongoDB database for documents that match specific criteria (e.g., find all users aged between 20 and 30). Display the results.

c) Create a Python script that updates a document in a MongoDB collection. For example, modify the email address of a user based on their name. Display the updated document after the modification.

13. MongoDB :

a) Write a Python script to connect to a MongoDB database and insert documents into a collection.

b) Implement CRUD operations (Create, Read, Update, Delete) using PyMongo library on a MongoDB collection.

c) Develop a Flask application that interacts with MongoDB to store and retrieve user data (e.g., user profiles, blog posts).

SYLLABUS

SEMESTER-II

Course Code:CSAI8126	Course Title: **ADVANCED OPERATING SYSTEM CONCEPTS WITH LINUX**
Course Credits: 04	Hours/Week: 04
Total Contact Hours: 52	Formative Assessment Marks: 50
Exam Marks: 50	Exam Duration: 2 Hrs

Course Outcomes (COs)

CO1: Explain the fundamental concepts of Operating Systems, including components, services, system calls, protection, security mechanisms, and different computing environments.
CO2: Apply Linux utilities and shell programming concepts using Bash, Sed, and Awk for file handling, process management, text processing, automation, and system administration tasks.
CO3: Analyze distributed operating system concepts such as communication primitives, logical and vector clocks, causal ordering, distributed mutual exclusion, deadlock detection, and agreement protocols.
CO4: Evaluate distributed resource management and fault tolerance techniques including distributed file systems, distributed shared memory, scheduling algorithms, checkpointing, recovery, and commit protocols.
CO5: Assess the design and operation of multiprocessor and database operating systems, focusing on process synchronization, scheduling, memory management, reliability, and concurrency control algorithms

Unit- wise Syllabus

Unit	Title	No. of hours
I	**OPERATING SYSTEM** Introduction,Components of Operating System, Operating System Operations, Protection and	12

	Security. Computing Environment. Abstract View of OS: User view, System View, Operating System Services, System Calls: Concept, Types of System Calls Linux Architecture,Process model.	
II	**SHELL PROGRAMMING IN LINUX** Linux Utilities - File handling utilities, Security by file permissions, Process utilities, Disk utilities, Networking commands, Filters, Text processing utilities and Backup utilities. SedScripts, Operation, Addresses, Commands, Applications, awk- Execution, Fields and Records, Scripts, Operation, Patterns, Actions, Associative Arrays, String and Mathematical functions, System commands in awk, Applications. Shell programming with Bourne again shell(bash) - Introduction, shell responsibilities, pipes and Redirection, here documents, running a shell script, the shell as a programming language, shell meta characters, file name substitution, shell variables, command substitution, shell commands, the environment, quoting, test command, control structures, arithmetic in shell, shell script examples, interrupt processing, functions, debugging shell scripts. Introduction to VI Editor	12
III	**DISTRIBUTED OPERATING SYSTEMS** Introduction – Issues – Communication network and Primitives, – Theoretical Foundations: Inherent Limitations - Lamport's Logical Clock; Vector Clock; Causal Ordering; Global State; Termination Detection. Distributed Mutual Exclusion Non-Token Based Algorithms – Lamport's Algorithm - Token-Based Algorithms Suzuki-Kasami's Broadcast Algorithm – Distributed Deadlock Detection – Issues Centralized Deadlock-Detection Algorithms - Distributed Deadlock-Detection Algorithms. Agreement Protocols – Classification (two)- Solutions(two) –Applications.	12

IV	**DISTRIBUTED RESOURCE MANAGEMENT AND FAULT TOLERANCE** Distributed File systems – Architecture – Mechanisms – Design Issues – Distributed Shared Memory – Architecture – Algorithm(two) – Protocols - Design Issues. Distributed Scheduling – Issues – Components(two) – Algorithms (two). Basic Concepts-Classification of Failures – Basic Approaches to Recovery; Recovery in Concurrent System; Synchronous and Asynchronous Check pointing and Recovery; Check pointing in Distributed Database Systems; Fault Tolerance; Issues - Two-phase and Non blocking Commit Protocols; Voting Protocols; Dynamic Voting Protocols.	12
V	**MULTIPROCESSOR AND DATABASE OPERATING SYSTEMS** Structures – Design Issues – Threads – Process Synchronization – Processor Scheduling Memory Management – Reliability / Fault Tolerance(two); Database Operating Systems – Introduction – Concurrency Control – Distributed Database Systems – Concurrency Control Algorithms(two).	12

TEXT BOOKS:

1. Andrew S. Tanenbaum, Herbert Bos, "Modern Operating Systems, 5th Edition", Pearson, 2022.
2. Abraham Silberschatz, Peter B. Galvin, Greg Gagne, "Operating System Concepts, 10th Edition", John Wiley & Sons, Inc., 2021.
3. Silberschatz, Galvin, Greg, “Operating System Concepts”, Wiley and Sons, 9th Edition, 2015.
4. Sumitabha Das, “Unix concept and Programming”, McGraw Hill education, 4th Edition, 2015.

REFERENCE BOOKS:

1. William Stallings, "Operating Systems: Internals and Design Principles, 9th (or 10th) Edition", Pearson, 2021.
2. Dhananjay M. Dhamdhere, "Operating Systems: A Concept-Based Approach, 3rd Edition", McGraw Hill Education, 2017.
3. Kenneth H. Rosen, Douglas Host, Rachel Klee, et al., "UNIX: The Complete Reference, 6th Edition", McGraw-Hill/Osborne, 2017.

Course Code	CSAI8226
Course Title	**Cryptography Techniques**
Course Credit	4
Total Contact Hours	60 Hrs.

Course Outcomes (COs)

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

CO1: Understand the fundamental concepts, goals, and mathematical foundations of cryptography.

CO2: Analyze and apply classical and symmetric key cryptographic techniques.

CO3: Understand and implement public key cryptographic algorithms and key exchange mechanisms.

CO4: Explain cryptographic hash functions, message authentication codes, and digital signatures.

CO5: Apply cryptographic techniques in secure communication protocols and emerging security applications.

Unit	Title	No. of hours
I	**Introduction to Cryptography & Mathematical Foundations** History and evolution of cryptography, Information security goals: confidentiality, integrity, authentication, non-repudiation, Cryptographic terminology: plaintext, ciphertext, keys, cryptanalysis, Introduction to symmetric vs asymmetric cryptography, Mathematical tools for cryptography: Modular arithmetic, Prime numbers and factorization, Greatest common divisor, Euclid's algorithm and Finite fields	12
II	**Classical and Modern Symmetric Cryptosystems** Classical ciphers: Caesar, Shift, Substitution, Transposition, Classical Cipher Attacks, Limitations of Classical Cryptosystems. Feistel cipher structure, Triple Data Encryption Standard (DES), Blow fish and Modes of operation: ECB – Electronic Codebook,CBC – Cipher Block Chaining,CFB – Cipher Feedback, OFB – Output Feedback, CTR – Counter Mode, GCM – Galois/Counter Mode	12
III	**Public-Key Cryptography (Asymmetric)**	12

	Principles of public-key cryptography, RSA algorithm: key generation, encryption/decryption, security assumptions, Diffie–Hellman Key Exchange, ElGamal Cryptosystem, Introduction to Elliptic Curve Cryptography (ECC)	
IV	**Cryptographic Hash Functions, MACs & Digital Signatures** Properties and applications of hash functions, MD5, SHA families (SHA-1, SHA-2, SHA-3), Message Authentication Codes (MAC), HMAC (Hash-based Message Authentication Code), Digital signatures: principles and verification and Comparison of signature schemes.	12
V	**Key Management Protocols** Key distribution and management techniques, Public Key Infrastructure (PKI) and certificates, Authentication protocols (Kerberos) Secure communication protocols, Basics of Quantum Cryptography, QKD Protocols, Quantum Key Distribution (QKD), Introduction to post-quantum cryptography, Algorithms and Real-world applications (VPNs, secure email)	12

Textbooks

1. William Stallings — *Cryptography and Network Security: Principles and Practice*
   • Comprehensive, widely adopted for academic courses. Slow introduction from basics to advanced protocols.
2. Jonathan Katz & Yehuda Lindell — *Introduction to Modern Cryptography*
   • Strong theoretical foundation with modern formal approaches and proofs.

Reference Books

1. Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd Edition (20th Anniversary Edition), 2015.
2. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, *Handbook of Applied Cryptography*, 1st Edition, 1996.
3. Christof Paar & Jan Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*, 1st Edition, 2010.
4. Behrouz A. Forouzan & Debdeep Mukhopadhyay, *Cryptography and Network Security*, 3rd Edition, 2015.

Course Code: CSAI8326	Course Title: **Cloud Security**
Course Credits: 04	Hours/Week: 04
Total Contact Hours: 52	Formative Assessment Marks: 50
Exam Marks: 50	Exam Duration: 2 Hrs

Course Outcomes (COs)

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

CO1: Explain cloud computing fundamentals, service/deployment models, architectures, vulnerabilities, cloud security concepts and standards.

CO2: Analyze cloud security goals and privacy issues including CIA triad, access control, identity management, SLA, and compliance requirements.

CO3: Identify threat models, cloud attack taxonomies, and classify intrusion detection systems and techniques used in cloud environments.

CO4: Apply cloud attack and security tools, including VM, VMM, and network-level tools, and analyze real-world case studies such as LibVMI.

CO5: Evaluate virtual machine, hypervisor, and container security mechanisms and propose suitable defense strategies for practical cloud scenarios.

Unit- wise Syllabus

UNIT	TITLE	No. of Hours
I	**Cloud Computing and Security Fundamentals:** **Introduction to Cloud Computing**, SPI Framework, Cloud Service models, Cloud Deployment Models, Cloud Service Platforms, Cloud Reference Architecture. Vulnerabilities present in cloud, Need of cloud security, **Cloud Security Concepts:** Multi-tenancy, Virtualization, Data outsourcing, Trust management, Metadata security. **Cloud Security Standards:** Control objectives for information and related technology (COBIT), ISO/IEC20000, Cloud security alliance (CSA) cloud controls matrix, CSA Cloud Reference Model, NIST Cloud Reference Model.	10
II	**Cloud Security and Privacy Issues:** **Cloud Security Goals / Concepts:** Confidentiality, Integrity, Availability (CIA triad), Authentication, Authorization, Auditing and Access control. **Cloud Security Issues:** Application-level security issues, Network level security issues, Virtualization level security issues, Data security, Identity management and access control, Improper cryptographic keys management, Service level agreement (SLA), Regular audit and compliances, Cloud and CSP migration, SLA and trust level issues, and Hardware-level security issues. **Security Requirements for Privacy:** Fine-grained access control, Privacy-preserving and Collision resistance. Privacy Issues in Cloud: Defining roles to actors, Compliance, Legal issues and multi-location issues, Privacy issues on CIA, Protection of the data, User control lacking and Data movement.	**12Hrs**
III	**Threat Model, Cloud Attacks, and Intrusion detection Techniques:** **Threat Model:** Type of attack entities, Attack surfaces with attack scenarios. A Taxonomy of Attacks: VMAT, VMMAT, HWAT, VSWAT and TENAT	**12Hrs**

	Classification of Intrusion Detection Systems in Cloud: TVM-based Intrusion Detection System. Hypervisor-based Intrusion Detection System. Network-based Intrusion Detection System. Distributed Intrusion Detection Systems. **Intrusion Detection Techniques in Cloud:** Misuse detection techniques, Anomaly detection techniques, Virtual machine introspection (VMI) techniques, Hypervisor introspection-based techniques, and Hybrid techniques. **Case Study:** Description of Features for Attack Analysis Based on Dataset including Fuzzers, Analysis, Backdoor, Exploits, Generic, Reconnaissance, Shellcode, and Worms.	
IV	**Cloud Attack and Security Tools:** **Attack Tools:** Network-level attack tools, VM-level attack tools, and VMM attack tools. **Security Tools :** Network security tools, VM security tool, and VMM security tools. **Case Study of LibVMI:** A Virtualization-Specific Tool including Check the system configurations, Install KVM and necessary dependencies, Creating a virtual machine, Install LibVMI tool and necessary dependencies	**8 Hrs**
V	**Virtual Machine, Hypervisor and Container Security:** **Virtual Machine Introspection (VMI):** VM hook based, VM-state information based, Hypercall verification based, Guest OS kernel debugging based, and VM interrupt analysis based. Hypervisor Introspection (HVI): Nested virtualization, Code integrity checking using hardware-support, Memory integrity checking using hardware/software support, Revisiting the VMM design, and VM-assisted hypervisor introspection. **Container Security:** Threat Model in Containerized Environment including Attacks in containers. Defense Mechanisms. **Case Study:** SQL Injection Attack in Containers.	**10 Hrs**

Text Book:

1.Cloud Security: Attacks, Techniques, Tools and Challenges, Preeti Mishra, Emmanuel S. Pilli, R. C. Joshi, 1st Edition, CRC Press, 2024.

Reference Books:

1.Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Ronald L. Krutz, Russell Dean Vines, 1st Edition, Wiley Publishing, 2010.
2.Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, Tim Mather, Subra Kumaraswamy, Shahed Latif, 1st Edition, O'Reilly Media, 2009.
3.Cloud Computing Security: Strategies and Best Practices, N. Agrawal, R. Kumar, S. Tapaswi, 1st Edition, CRC Press / Routledge, 2024.

Course Code: CSAI8426	Course Title: **Machine Learning Essentials**
Course Credits: 04	Hours/Week: 04
Total Hours: 60	Formative Assessment Marks: 50
Exam Marks: 50	Exam Duration: 2 Hrs

Course Outcomes:

CO1: Identify the basic concepts of Machine Learning and Training models.
CO2: Identify and apply the appropriate machine learning techniques for classification.
CO3: Analyze and apply unsupervised learning techniques for solving real time problems.
CO4: Analyze the concept of Neural Network.
CO5: Analyze and apply the concepts of Markov Decision Process in HMM and Reinforcement Learning.

Unit- wise Syllabus

UNIT	TITLE	No of hours
I	**Introduction to Machine Learning:** Fundamentals of Machine Learning – Applications -Types of Machine Learning – Challenges of Machine Learning – Testing and Validating. Training a ML model-End-to-End Machine Learning Project – Working with Real Data – Get the Data – Explore and Visualize the Data – Prepare the Data for Machine Learning Algorithms, Cross- Validation and Resampling Method,Measuring Classifier Performance.	**12**
II	**Classification and Regression:** Supervised Learning- Regression –Linear Regression – Logistic Regression -Support Vector Machine – Naive Bayes – Decision Tree – KNN algorithm . **Case Study:** Loan Approval Prediction Using Decision Tree.	**12**
III	**Unsupervised Learning:** Introduction to clustering- Categories of Clustering-K-means clustering - Limits of K-means– Hierarchical clustering- agglomerative Clustering-Divisive Clustering-Expected maximization Algorithm. Dimensionality Reduction: Introduction, subset selection, principal component analysis(PCA) . **Case Study**: Customer Segmentation Using K-Means Clustering.	**12**
IV	**Artificial Neural Network:** Biological to Artificial Neurons – Logic Computations with Neurons – Perceptron - Multilayer Perceptron and Back propagation. **Case Study:** Handwritten Digit Recognition Using Multilayer Perceptron (MLP).	**12**
V	**Hidden Markov Models and Reinforcement Learning:** Definition of Markov Processes, The Hidden Markov Model Structure-Hidden states vs observed variables, Transition and emission probabilities, Initial state distributions, Key Problems in HMMs-Computing the probability of an observed sequence, Inferring most likely hidden state sequences (e.g.,	**12**

	Viterbi algorithm), Estimating model parameters (e.g., Baum-Welch algorithm/MM algorithm) . Introduction to Reinforcement Learning- Formalizing agents, environments, actions, rewards, Distinction from supervised/unsupervised learning. **Case Study:** Speech Recognition Using Hidden Markov Models (HMMs).	

Text Book(s):

1. Ethem Alpaydin, “Introduction to Machine Learning”, 2020, Fourth Edition, MIT Press.
2. Aurelien Geron, “Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow”, 2019, 2nd Edition,O'Reilly Media, Inc.

Reference Books:

1. Stephen Marsland, “Machine Learning: An Algorithmic Perspective “,2014, Second Edition”, CRC Press.
2. Tom M. Mitchell, “Machine Learning”,2021,by McGraw-Hill.

Course Code: CSAI8526	Course Title: **Big Data Analytics**
Course Credits: 04	Hours/Week: 04
Total Contact Hours: 52	Formative Assessment Marks: 50
Exam Marks: 50	Exam Duration: 2 Hrs

Course Outcomes:

CO1: Understand the concept of big data and its challenges, describe the role of Hadoop in handling big data, explain the basic workflow of processing big data using Hadoop.

CO2: Comprehend the architecture and components of Hadoop Distributed File System (HDFS), understand the MapReduce programming model and its role in processing large datasets.

CO3: Apply Python for streaming data processing in a Hadoop environment, Implement MapReduce jobs using Python for data analysis tasks, demonstrate the ability to count bigrams in a dataset using MapReduce, provide an overview of Pig for implementing machine learning techniques in big data analytics.

CO4: Use Hive for querying and analyzing structured data in Hadoop, describe the role of HBase in storing and retrieving large volumes of data in Hadoop, utilize MySQL for integrating relational databases with Hadoop, explain the use of Flume for ingesting streaming data into Hadoop for analysis.

CO5: Analyze real-world case studies to understand the application of Spark in big data analytics, demonstrate the ability to use Spark for processing and analyzing large datasets, apply machine learning algorithms in Spark for predictive analytics.

Unit- wise Syllabus

Unit	Title	No. of hours
I	**Introduction to Big Data and Hadoop** Introduction To Big Data Platform, Challenges Of Conventional Systems, Web Data, Evolution of Analytic Scalability, Analytic Processes, and Tools. Data Product, Building Data Products at Scale with Hadoop, Leveraging Large Datasets, Hadoop for Data Products, The Data Science Pipeline and the Hadoop Ecosystem, Big Data Workflows.	**12**
II	**Hadoop Distributed File System (HDFS)** Introduction to HDFS, Hadoop Architecture, A Hadoop Cluster - HDFS and YARN, Working with a Distributed File System, Basic File System Operations, File Permissions in HDFS, Other HDFS Interfaces. MapReduce: A Functional Programming Model, MapReduce implemented on a Cluster, Submitting a MapReduce Job to YARN.	**12**

III	**A Framework for Python and Hadoop Streaming** Hadoop Streaming, Computing on CSV Data with Streaming, Executing Streaming Jobs, Framework for MapReduce with Python, Counting Bigrams, Other Frameworks, Advanced MapReduce, Combiners, Partitioners, and Job Chaining. Pig, Pig Latin - Data Types, Relational Operators, User-Defined Functions. Machine learning - Collaborative Filtering, Classification, Clustering.	**12**
IV	**Structured Data Queries with Hive** The Hive Command-Line Interface (CLI), Hive Query Language (HQL), Data Analysis with Hive, HBase, NoSQL and Column-Oriented Databases, Real-Time Analytics with HBase, Importing Relational Data with Sqoop, Importing from MySQL to HDFS, Importing from MySQL to Hive, Importing from MySQL to HBase, Ingesting Streaming Data with Flume, Flume Data Flows, Ingesting Product Impression Data with Flume.	**12**
V	**Big Data with Spark** Spark Introduction - Why Spark?, The Spark Stack, Understanding Spark Cluster Modes on YARN, RDDs (Resilient Distributed Datasets), RDD lineage, General RDD Operations, Building a Spark Application (Java, Python), The Spark Application Web UI, Configuring Spark Properties, Running Spark on Cluster, RDD Partitions, Spark SQL and DataFrames, Common Spark Use Cases(Data Cleaning (Movielens))	**12**

Textbook:

- Data Analytics with Hadoop by Benjamin Bengfort, Jenny Kim, 2016, O'Reilly Media, Inc.

Reference books:

- Taming The Big Data Tidal Wave: Finding Opportunities in Huge Data Streams with Advanced Analytics, Bill Franks, Thomas H. Davenport, 2012.
- Practical Data Science with Hadoop and Spark: Designing and Building Effective Analytics at Scale, 1st edition, Addison-Wesley Professional, 2017.
- E. Capriolo, D. Wampler, and J. Rutherglen, "Programming Hive", O'Reilley, 2012.
- Alan Gates, "Programming Pig", O'Reilley, 2011.

Course Code	CSAI8P126
Course Title	**Cryptography Techniques Lab**
Course Credit	02

Course Outcomes (COs)

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

- **CO1:** Implement classical cryptographic algorithms for secure data transformation.
- **CO2:** Design and implement symmetric key cryptographic algorithms and modes of operation.
- **CO3:** Implement public key cryptographic algorithms and key exchange mechanisms.
- **CO4:** Apply cryptographic hash functions, MACs, and digital signatures for authentication.
- **CO5:** Demonstrate secure communication protocols and real-world cryptographic applications.

List of Experiments / Programs:

1. Program to implement Caesar Cipher (encryption and decryption).
2. Program to implement Monoalphabetic Substitution Cipher.
3. Program to implement Transposition Cipher.
4. Program to implement DES encryption and decryption.
5. Program to implement AES encryption and decryption.
6. Program to demonstrate Block Cipher Modes of Operation (ECB, CBC).
7. Program to perform file encryption using a symmetric key algorithm.
8. Program to implement RSA algorithm (key generation, encryption, decryption).
9. Program to implement Diffie–Hellman Key Exchange.
10. Program to implement ElGamal Cryptosystem.
11. Program to demonstrate Elliptic Curve Cryptography (ECC) basics.
12. Program to generate hash values using MD5 and SHA-256.
13. Program to implement Message Authentication Code (MAC).
14. Program to implement HMAC using SHA-256.
15. Program to demonstrate Digital Signature creation and verification.
16. Program to demonstrate Secure File Transfer using Cryptography.
17. Program to simulate Public Key Infrastructure (PKI) concepts.
18. Program to demonstrate the SSL/TLS handshake process (simulation).

19. Case study / mini project on Secure Communication System

Course Code: **CSAI8P226**	Course Title: **Machine Learning Lab**
Course Credits: 03	Hours/Week: 06
Total Contact Hours: 66	Formative Assessment Marks: 50
Exam Marks: 50	Exam Duration: 2 Hrs

Course Outcomes (COs)

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

CO1: Understand the library functions in python for data preprocessing
CO2: Use the python machine learning models.
CO3: Understand complexity of Machine Learning algorithms and their limitations
CO4: Apply appropriate algorithms for problem solving.
CO5: Capable of performing experiments in Machine Learning using real-world data

Program List	
	Python Libraries: Numpy, Pandas, MatplotLib and Scikit
1.	Creating Arrays and Array Operations: a) Create a 1D array with elements from 0 to 9. b) Create a 2D array with shape (3, 4) filled with random numbers. c) Calculate the mean and standard deviation of a given array. d) Normalize the values of an array (subtract the mean and divide by the standard deviation).

<table>
<tr><td>2</td><td>Generating Array, Reshaping and Stacking:
a) Create a 1D array of 10 evenly spaced values between 0 and 1.
b) Generate a 3x3 identity matrix.
c) Reshape a 1D array into a 2D array with shape (2, 5).
d) Stack two arrays vertically and horizontally.</td></tr>
<tr><td>3</td><td>Indexing and Slicing & Matrix Operations:
a) Extract the third column from a 2D array.
b) Reverse the order of elements in a 1D array.
c) Create two matrices (2x3 and 3x4) and perform matrix multiplication.
d) Find the determinant of a 3x3 matrix.</td></tr>
<tr><td>4</td><td>Statistical Operations, Broadcasting:
a) Generate a random 2D array and calculate the mean along each axis.
b) Find the minimum and maximum values in a given array.
c) Create a 1D array and add a constant value to each element without using a loop.
d) Multiply each row of a 2D array by a different constant.</td></tr>
<tr><td>5</td><td>Develop a python program to create pandas data frame from list of data.</td></tr>
<tr><td>6</td><td>Develop a python program to analyze the dataset using pandas and matplotlib library</td></tr>
<tr><td>7</td><td>Develop a program to compute Mean, Median, Mode, Variance and Standard Deviation using Datasets.</td></tr>
<tr><td>8</td><td>Plot histogram for the given dataset.
<table>
<tr><td>10-15</td><td>15-20</td><td>20-25</td><td>25-30</td><td>30-35</td></tr>
<tr><td>5</td><td>6</td><td>9</td><td>8</td><td>2</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td>9</td><td>Draw box-and-whisker plot for the data set {3, 7, 8, 5, 12, 14, 21, 13, 18}.</td></tr>
<tr><td>10</td><td>Draw Line Plot and Bar chart for the following data.
<table><tr><td>Elapsed time (s)</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td></tr><tr><td>Speed(m/s)</td><td>0</td><td>3</td><td>7</td><td>12</td><td>20</td><td>30</td><td>45.6</td></tr></table></td></tr>
<tr><td>11</td><td>Implement and demonstrate the FIND-S algorithm for finding the most specific hypothesis based on a given set of training data samples. Read the
training data from a .CSV file</td></tr>
<tr><td>12</td><td>Develop a python program to implement Simple linear regression and plot
the graph</td></tr>
<tr><td>13</td><td>Develop a python program to implement single layer perceptron.</td></tr>
<tr><td>14</td><td>Implement the naïve Bayesian classifier for a sample training data set stored as a .CSV file. Compute the accuracy of the classifier, considering
few test data sets.</td></tr>
<tr><td>15</td><td>Demonstrate the working of the decision tree based ID3 algorithm. Use an appropriate data set for building the decision tree and apply this knowledge
to classify a new sample.</td></tr>
<tr><td>16</td><td>Implement k-Nearest Neighbor algorithm to classify the iris data set. Print
both correct and wrong predictions.</td></tr>
<tr><td>17</td><td>Apply k means algorithm to cluster a set of data stored in a .CSV file.</td></tr>
<tr><td>18</td><td>Build an Artificial Neural Network by implementing the Back propagation
algorithm and test the same using appropriate data sets.</td></tr>
<tr><td>19</td><td>Write a Python program to Read a CSV file,Handle missing values,</td></tr>
</table>

	Apply StandardScaler,Split the data into training and testing sets
20	Implement a program to split a dataset into **70:30** ratio and compute: Accuracy,Precision,Recall,F1-score
21	Write a Python program to compute and display a confusion matrix for a given classifier.
22	Implement SVM for a linearly separable dataset and visualize the decision boundary.
23	Implement PCA to reduce the dataset to two dimensions and visualize the transformed data.
24	Apply Agglomerative Hierarchical Clustering and plot the dendrogram.

****