ಮಂಗಳೂರು ವಿಶ್ವವಿದ್ಯಾನಿಲಯ

MANGALORE UNIVERSITY

(Accredited by NAAC)

ಕ್ರಮಾಂಕ/ No. : MU/ACC/CR 3/2023-24/A2

ಕುಲಸಚಿವರ ಕಛೇರಿ
ಮಂಗಳಗಂಗೋತ್ರಿ – 574 199
Office of the Registrar
Mangalagangothri – 574 199
ದಿನಾಂಕ/Date:10.10.2023

NOTIFICATION

Sub: Revised syllabus of Career Oriented Programme in Artificial Intelligence , Big Data Analytics and Cyber Security

Ref: Academic Council approval vide agenda No.: ಎಸಿಸಿ:ಶೈ.ಸಾ.ಸ.2:24(2023–24) dtd 04.10.2023.

*****

The revised syllabus of Career Oriented Programme in Artificial Intelligence, Big Data Analytics and Cyber Security which is approved by the Academic Council at its meeting held on 04.10.2023 is hereby notified for implementation with effect from the academic year 2023-24 and onwards.

Copy of the Syllabus shall be downloaded from the University Website (www.mangaloreuniversity.ac.in)

REGISTRAR

To

1. The Registrar (Evaluation), Mangalore University.
2. The Chairman, UG BOS in Computer Science and Computer Applications, Dept. of Computer Science, Mangalore University.
3. The Principals of the College Concerned.
4. The Superintendent (ACC), O/o the Registrar, Mangalore University.
5. The Asst. Registrar (ACC), O/o the Registrar, Mangalore University.
6. The Director, DUIMS, Mangalore University – with a request to publish in the website.
7. Guard File.

UGC CAREER ORIENTED COURSE ON

ARTIFICIAL INTELLIGENCE, BIG DATA ANALYTICS AND CYBER SECURITY

Preamble:

In a world increasingly defined by technological advancements and digital transformation, the study of Artificial Intelligence has emerged as a transformative force that redefines the boundaries of human potential. The Artificial Intelligence and Machine Learning degree program at Mangalore University is born out of the conviction that AI is not merely a field of study but a revolutionary endeavour poised to reshape industries, societies, and the very fabric of human existence. The mission is to cultivate a community of innovators, problem solvers, and visionaries who harness the power of AI to address complex challenges, drive innovation, and unlock new opportunities for a better future. At the heart of our program lies a commitment to excellence, ethics, and the pursuit of knowledge that transcends disciplinary boundaries.

On the other hand, in the era of data-driven decision-making and transformative technological advancements, the study of Machine Learning has emerged as an indispensable discipline that empowers individuals to extract knowledge, patterns, and insights from data. The program is founded on the belief that machine learning is not merely a field of study but a powerful force that drives innovation, shapes industries, and unlocks the potential for a smarter, more interconnected world. We aim to cultivate a community of learners, researchers, and innovators who harness the power of machine learning to address complex problems, fuel innovation, and contribute to the advancement of science and society. Our program embodies a commitment to academic excellence, ethics, and the pursuit of knowledge at the forefront of machine learning.

Artificial Intelligence (AI) and Machine Learning (ML) have experienced tremendous growth in recent years, leading to a wide range of job opportunities across various industries. Some of the prominent job roles and career opportunities in the field of AI and ML include Machine Learning Engineer, Data Scientist, Computer Vision Engineer, Natural Language Processing (NLP) Engineer, Data Engineer, AI/ML Solutions Architect, Robotics Engineer, AI for Healthcare Specialist, AI in Finance Analyst, AI in Cyber security Analyst, AI in Marketing Analyst, etc. Job opportunities in AI and ML are diverse and continue to expand as businesses and industries increasingly adopt these technologies. The demand for skilled professionals in this field is expected to remain high in the coming years.

Data analysis is of paramount importance in various fields and industries due to its numerous benefits and contributions. Data analysis is a versatile and indispensable tool in today's data-driven world. It empowers individuals, organizations, and governments to make informed decisions, improve processes, and drive innovation across various domains. Data analysis is useful for better planning and forecasting, performing risk management, marketing optimization, quality improvement, fraud detection, etc. In this context, this course will be of significance to the student community for better employability in industry sectors.

Cyber security is of paramount significance in today's digitally interconnected world due to the protection of sensitive data, prevention of data breaches, financial stability, national security, protection of intellectual property, privacy preservation, maintaining trust, etc. Cyber security is essential for protecting individuals, businesses, governments, and society as a whole from the growing threats in the digital age. Its significance extends to financial stability, national security, privacy, and the preservation of trust and data integrity in an increasingly interconnected world. The field of cyber security has created a vast number of job opportunities, contributing to economic growth and job security. As cyber threats continue to evolve, there is a growing demand for cyber security professionals. The field of cyber security offers a wide range of job opportunities due to the increasing importance of protecting digital assets and information in today's interconnected world. Some of the most common and sought-after job roles in cyber security include cyber security analyst, security consultant, security engineer: penetration tester (ethical hacker), compliance officer/auditor, forensic analyst, threat intelligence analyst: block chain security expert and many more.

Course objectives:

The objectives of this career oriented course can vary depending on the level of the course (certificate, diploma and advanced diploma). However, some common objectives are as follows:

Artificial Intelligence:

- To provide students with a comprehensive understanding of the fundamental concepts, theories, and principles of artificial intelligence and machine learning.
- To equip students with the practical skills necessary to develop, implement, and evaluate machine learning algorithms and AI systems.
- To enable students to effectively collect, pre-process, and analyse large and complex data sets for AI and ML applications.

- To foster students' ability to apply AI and ML techniques to solve real-world problems across diverse domains, including healthcare, finance, robotics, and natural language processing.
- To encourage collaboration across disciplines and departments, recognizing that AI and ML intersect with various fields, including computer science, mathematics, psychology, and economics.
- To promote a culture of research and innovation, enabling students to contribute to the advancement of AI and ML through research projects and initiatives.
- To provide opportunities for students to demonstrate their mastery of AI and ML concepts through capstone projects that tackle complex, real-world challenges.
- To prepare students for a wide range of career opportunities in academia, research, industry, and entrepreneurship within the AI and ML field.
- To encourage students to actively engage with the AI and ML community, participate in conferences, workshops, and hackathons, and contribute to open-source projects.

Big Data Analysis:

- Gain a fundamental understanding of key data concepts, such as data types, data structures, data collection methods, and data sources.
- Learn how to clean and pre-process data to ensure its quality and suitability for analysis.
- Develop skills in EDA techniques to explore and visualize data, identify patterns, trends, and outliers, and gain insights that can inform further analysis.
- Acquire skills in data visualization to effectively communicate insights and findings through charts, graphs, and interactive dashboards.
- Familiarize with data analysis software and tools such as Python, R, Excel, and data visualization libraries (e.g., Matplotlib, ggplot2, Tableau).
- Understand the ethical considerations and privacy concerns related to data analysis, including issues of consent, data anonymization, and responsible data handling.
- Learn project management skills specific to data analysis, including data project planning, data collection, analysis, and reporting.
- Provide opportunities for hands-on practice with real datasets and projects to reinforce theoretical knowledge.

Cyber Security:

- Understand procedures to protect sensitive data from unauthorized access, disclosure, or theft.
- Process to verify the identity of users, devices, or systems attempting to access resources.

- How to determine what actions or resources users, devices, or systems are permitted to access after authentication.
- Implementation of encryption and other security measures to protect data at rest, in transit, and during processing.
- Know about monitoring systems and networks for signs of suspicious or malicious activity.
- Identify and address vulnerabilities in systems, software, and configurations to reduce the attack surface and minimize the risk of exploitation.
- Develop and enforce security policies and procedures that define acceptable behaviour, access controls, and security requirements within an organization.
- Security Testing and Assessment: Conduct regular security assessments, penetration testing, and vulnerability scanning to identify weaknesses and gaps in security defences.

Scheme of the course:

FIRST YEAR (LEADING TO CERTIFICATE)

Paper	Instruction (Hr.)	Duration of Examination (Hr.)	Marks for Final Exam	Marks for Internal Exam	Total Marks
CAIDACS Paper-I	03	03	100	50	150
Practical-I	03	03	100	50	150

SECOND YEAR (LEADING TO DIPLOMA)

Paper	Instruction (Hr.)	Duration of Examination (Hr.)	Marks for Final Exam	Marks for Internal Exam	Total Marks
CAIDACS Paper-II	03	03	100	50	150
Practical-II	03	03	100	50	150

III YEAR (LEADING TO ADVANCED DIPLOMA)

Paper	Instruction (Hr.)	Duration of Examination (Hr.)	Marks for Final Exam	Marks for Internal Exam	Total Marks
CAIDACS Paper-III	03	03	100	50	150
Practical-III	03	03	100	50	150
Project	03	--	100	--	100

Every student is expected to take up a project work under a guide relating to the areas of their study and submit a report containing detailed discussion about the project which will have two valuations (1 internal and 1 external) for a maximum of 50 marks. A viva voce examination is to be conducted based on their project report by the external examiner/examiners for a maximum of 50 marks.

Pedagogy:

- Tutorial and Group Discussion
- Practical Experience
- Projects and Assignments
- Course Presentation
- Industrial Visit
- Seminars and Workshops

FIRST YEAR:

CAIDACS PAPER-I:

1. Introduction to Artificial Intelligence and Problem-Solving Agent: Problems of AI, Intelligent Agents, Agents & environment, nature of environment, structure of agents, goal-based agents, utility-based agents, learning agents. Defining the problem as state space search, production system, problem characteristics
2. Search Techniques: Problem solving agents, searching for solutions; uniform search strategies: breadth first search, depth first search. Heuristic search strategies Greedy best - first search, A* search.
3. Python Basics: Python Data Structures, Python Programming Fundamentals, Conditions and Branching, Loops, Functions, Python Packages, Working with NUMPY, Working with Pandas, Introduction to Data Visualization, Introduction to Matplotlib and Seaborn, Basic Plotting with Matplotlib and Seaborn
4. Introduction to Data Analysis: Introduction to data analysis and its importance, Types of data (categorical, numerical, ordinal), Data sources and data collection methods.
5. Data Cleaning and Pre-processing: Data cleaning techniques-handling missing data, outliers; Data pre-processing: data normalization, scaling.
6. Introduction to data visualization: Types of charts and graphs (bar charts, histograms, scatter plots), Data visualization tools
7. Introduction to Cyber security: Definition, Importance of cyber security, Key cyber security concepts and terminology, Ethical and legal aspects of cyber security
8. Cyber Threats and Attack Vectors: Common cyber threats (e.g., malware, phishing, ransomware, Attack vectors and techniques, Case studies of notable cyber attacks

Text Books:

- Russell, Norvig, Artifificial Intelligence: A Modern Approach, Third edition, Prentice Hall, 2010
- "Introduction to Data Science" by Jeffrey Stanton
- "Data Science for Business" by Foster Provost and Tom Fawcett.
- "Cyber security Essentials" by Charles J. Brooks

Practical-I

1. Write a Python Program to Print a Multiplication Table for the given number.
2. Write a Python Program to check whether the given number is prime or not.
3. Write a Python Program to display the Fibonacci series for a given number.
4. Write a menu driven program to convert the given temperature from Fahrenheit to Celsius and vice versa depending upon user's choice.
5. Write a Python Program to implement List Operations (Nested List, Length, Concatenation, Membership, Iteration, Indexing and slicing).
6. Write a Python Program to Transpose the Matrix.
7. Write a Python Program to implement the List Methods (Add, Append, Extend & Delete)
8. Write a Python Program to implement the Breadth first Search Traversal.
9. Write a Python Program to Find factorial of the given number
10. Write a Python Program to implement the simple chat bot.
11. Analyse a dataset of stock prices to identify trends and patterns.
12. Clean and pre-process a dataset with missing values, outliers, and inconsistencies.
13. Normalize and scale features in a dataset for analysis.
14. Create visualizations (e.g., bar charts, histograms, scatter plots) to represent data distributions and relationships.
15. Visualize the geographical distribution of COVID-19 cases using maps.
16. Choose a specific dataset (e.g., global GDP, COVID-19 statistics) and create informative data visualizations.
17. Identify phishing emails and distinguish them from legitimate messages.
18. Set up a controlled environment (sandbox) for analyzing malware samples.
19. Analyze and identify characteristics of different types of malware (e.g., viruses, Trojans, ransomware).
20. Analyze phishing URLs for malicious intent.

SECOND YEAR:

CAIDACS PAPER-II:

1. Knowledge representation issues, predicate logic- logic programming, semantic nets-frames and inheritance, constraint propagation, representing knowledge using rules, rules based deduction systems. Review of probability, Baye's probabilistic interferences and Dempster Shafer theory.
2. First order logic. Inference in first order logic, propositional vs. first order inference, unification & lifts forward chaining, Backward chaining, Resolution, Statistical Learning methods, Reinforcement Learning.
3. Machine Learning Fundamentals: Introduction to machine learning, Supervised, unsupervised, and reinforcement learning, Simple Linear regression, Decision trees
4. Clustering: Distance measures, Different clustering methods -Distance, Density, Hierarchical, Iterative distance-based clustering, Dealing with continuous, categorical values in K-Means, Introduction to Naïve Bayes Classifier and Support Vector Machines.

5. Descriptive Statistics: Measures of central tendency (mean, median, mode), Measures of variability (range, variance, standard deviation, Percentiles and quartiles; Probability and Distributions: Basic probability concepts, Probability distributions (normal, binomial, Poisson), Sampling and the Central Limit Theorem.
6. Security Principles and Practices: Security principles (confidentiality, integrity, availability), Defense-in-depth and layered security, Security policies and best practices
7. Network Security: Network security fundamentals, Firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS), Virtual Private Networks (VPNs) and secure network design.
8. Cryptography and Data Protection: Basics of cryptography, Encryption algorithms and protocols, Public key infrastructure (PKI) and digital certificates.

Text Books:

- Tom Mitchell, "Machine Learning", McGraw Hill, 1997.
- E. Alpaydin, "Introduction to Machine Learning", PHI, 2005.
- Andrew Ng, Machine learning yearning, https://www.deeplearning.ai/machine-learningyearning/
- AurolienGeron, "Hands-On Machine Learning with Scikit-Learn and TensorFlow, Shroff/O'Reilly",2017.
- Andreas Muller and Sarah Guido, "Introduction to Machine Learning with Python: A Guide for Data Scientists", Shroff/O'Reilly, 2016.
- Russell, Norvig, Artifificial Intelligence: A Modern Approach, Third edition, Prentice Hall,2010
- Michael Nielsen, "Neural Networks and Deep Learning", Goodreads (eBook), 2013.
- "Introduction to Data Science" by Jeffrey Stanton
- "Data Science for Business" by Foster Provost and Tom Fawcett.
- "Cyber security Essentials" by Charles J. Brooks
- "Introduction to the Practice of Statistics" by David S. Moore, George P. McCabe, and Bruce A. Craig.
- "Cyber security and Cyber war: What Everyone Needs to Know" by P.W. Singer and Allan Friedman

Practical-II:

1. Assuming a set of data that need to be classified, implement a decision tree model.
2. Implement the K-Means algorithm from scratch in Python
3. Apply K-Means to a synthetic dataset to understand the clustering process.
4. Use the scikit-learn to perform K-Means clustering on real-world datasets.
5. Implement hierarchical clustering algorithms like agglomerative or divisive clustering.
6. Apply hierarchical clustering to datasets with varying structures (e.g., single-linkage vs. complete-linkage clustering).
7. Implement a simple linear SVM classifier using scikit-learn or the SVM functions available in your chosen programming language.
8. Develop a linear SVM to a real-world dataset for binary classification.
9. Calculate descriptive statistics (e.g., mean, median, standard deviation) for a dataset.
10. Build a simple linear regression model to predict student test scores based on study time.
11. Identify suspicious or malicious network activity.
12. Install and configure antivirus and antimalware software.
13. Encrypt sensitive data using encryption tools or techniques.
14. Understand the principles of symmetric and asymmetric encryption.
15. Recognize social engineering tactics (e.g., phishing calls, pretexting) and respond appropriately.
16. Set up a home network with proper security measures (firewall, Wi-Fi encryption, strong router passwords).

THIRD YEAR

CAIDACS PAPER-III:

1. Software Agents Architecture for Intelligent Agents – Agent communication – Negotiation and Bargaining – Argumentation among Agents – Trust and Reputation in Multi-agent systems.
2. Ethical considerations in AI, Bias and fairness in AI algorithms, Guidelines for ethical AI development
3. Introduction to Neural networks, Learning rules and various activation functions, Single layer Perceptrons, Back Propagation networks, Architecture of Back propagation Networks, Back propagation Learning, Variation of Standard Back propagation Neural Network.
4. Characteristics of Big Data, Importance of Big Data Analytics, Applications of Big Data Analytics, Big Data Analytics process
5. Introduction to Hadoop ecosystem, Hadoop Distributed File System (HDFS), MapReduce programming model, Hadoop ecosystem components.
6. Security Risk Management: Risk assessment and analysis, Risk mitigation strategies, Security frameworks (e.g., NIST Cyber security Framework)
7. Access Control and Identity Management: Access control models (DAC, MAC, RBAC), Authentication and authorization, Identity and access management (IAM) solutions
8. Security Compliance and Regulations: Industry-specific regulations (e.g., HIPAA, GDPR), Compliance frameworks (e.g., ISO 27001), Legal and ethical considerations in cyber security

Text Books:

- Russell, Norvig, Artificial Intelligence: A Modern Approach, Third edition, Prentice Hall,2010
- Laurence Fausett, "Fundamentals of Neural Networks", Prentice Hall,1994
- "Introduction to Data Science" by Jeffrey Stanton
- "Data Science for Business" by Foster Provost and Tom Fawcett.
- "Introduction to the Practice of Statistics" by David S. Moore, George P. McCabe, and Bruce A. Craig.
- "Cyber security Essentials" by Charles J. Brooks
- "Cyber security and Cyber war: What Everyone Needs to Know" by P.W. Singer and Allan Friedman

Practical-III:

1. Develop a program to implement a basic feed forward neural network using a deep learning framework (e.g., Tensor Flow or PyTorch).
2. Develop a program to train the network on a synthetic dataset (e.g., XOR problem) to understand the basics of forward and backward propagation.
3. Configure a personal or network firewall to block or allow specific traffic.
4. Create firewall rules to protect a network from unauthorized access.
5. Capture and analyze network traffic using packet capture tools (e.g., Wireshark).
6. Perform regular scans and remove detected threats.
7. Configure web browsers for enhanced security and privacy.
8. Recognize and avoid potentially harmful websites.
9. Keep operating systems and software up to date by applying patches and updates.

10. Develop a patch management strategy.
11. Encrypt files before transferring or storing them in the cloud.
12. Practice secure file sharing and storage practices.
13. Secure a Wi-Fi network by changing default passwords, enabling encryption, and using strong pre-shared keys (PSKs).
14. Familiarize yourself with common security tools such as Nmap, Nessus, Snort, and OSSEC.

FINAL PROJECT

Students will work on an artificial intelligence/machine learning/data analysis/cyber security project using the skills learned throughout the course. Presentation of final projects and discussion.

Case Studies and Projects (tentative):

- Build a recommendation system for movies, books, or products using collaborative filtering or content-based filtering.
- Develop an AI agent that can play and excel in classic games like chess, Go, or video games like Flappy Bird.
- Create a diagnostic AI model that can predict diseases or conditions based on patient data like medical images, symptoms, and patient history.
- Build a stock price prediction model using time series analysis and sentiment analysis of news articles.
- Develop an AI system that can recognize and classify objects in images or videos.
- Create an image captioning system that generates descriptions for images.
- Build an AI system that can predict and mitigate the impact of natural disasters, such as earthquakes or hurricanes, using sensor data.
- Train a machine learning model to identify plant diseases from images, aiding in crop management.
- Create a machine learning model to predict creditworthiness based on customer data for a financial institution.
- Build a robot that can navigate its environment and perform tasks using computer vision and reinforcement learning.
- Develop a dashboard that provides real-time sentiment analysis of social media data for a brand or product.

- Create a fraud detection model for financial transactions to identify potentially fraudulent activities.
- Build a predictive model that forecasts patient hospital readmissions or disease progression.
- Work on data analysis such as analyzing and forecast monthly sales data for a retail store, Monitor and visualize data in real-time, etc.
- Work on a comprehensive data science capstone project that encompasses all stages of the data science process, from data collection to model deployment.
- Create a tool that assesses the strength of user passwords and provides recommendations for stronger passwords.
- Use network scanning tools like Nmap to scan your home network for open ports and vulnerabilities.
- Develop educational materials (e.g., presentations, pamphlets) to raise awareness about common cyber security threats and best practices.
- Configure a network firewall (e.g., pfSense, iptables).
- Test the firewall's effectiveness by simulating attacks and intrusion attempts.
- Monitor network traffic and detect suspicious or malicious activity.
- Design a secure network architecture for an organization, considering defense-in-depth principles.
- Build scripts or tools for automating security tasks (e.g., log analysis, vulnerability scanning).