COCHIN UNIVERSITY OF SCIENCE AND TECHNOLOGY

REGULATION, CURRICULUM & SYLLABUS

EXECUTIVE M. TECH IN COMPUTER SCIENCE AND ENGINEERING

(2025 Admissions Onwards)

DEPARTMENT OF COMPUTER APPLICATIONS COCHIN UNIVERSITY OF SCIENCE AND TECHNOLOGY KOCHI - 682022

VISION

To empower working professionals with advanced technical knowledge, leadership skills, and innovative problem-solving capabilities, enabling them to excel in their industries and contribute to transformative technological advancements on a global scale.

MISSON

1. To Provide Advanced Education: Deliver cutting-edge, industry-relevant technical knowledge and skills through a flexible and engaging learning environment tailored for working professionals.
2. To Foster Innovation: Encourage critical thinking and innovation by integrating research opportunities and practical industry applications in the curriculum.
3. To Develop Leadership: Cultivate leadership and strategic decision-making abilities to equip professionals for senior roles in technology-driven organizations.
4. To Promote Lifelong Learning: Inspire a culture of continuous learning and professional growth to adapt to evolving technologies and global challenges.
5. To Strengthen Industry-Academia Collaboration: Build robust partnerships with industries to ensure the curriculum addresses current challenges and prepares professionals for future opportunities.

1. PROGRAMME DESCRIPTION:

Executive Master of Technology in Computer Science and Engineering is a postgraduate degree program offered by Cochin University of Science and Technology (CUSAT) under the Department of Computer Applications. This two-year, four-semester program is primarily delivered online, offering working professionals and entrepreneurs an opportunity to enhance their expertise in computer science and engineering, while incorporating an essential offline laboratory component for practical experience. Upon successful completion, participants will be awarded the Executive MTech degree in Computer Science and Engineering by CUSAT.

2. PROGRAMME EDUCATIONAL OBJECTIVES (PEOS):

1. To enable graduates to analyse and solve complex computing challenges by applying mathematical and computer science principles with the aid of advanced computing tools.
2. To enable graduates to cultivate a research-oriented mindset in computer science, empowering them to pursue higher education and embrace lifelong learning and teaching.
3. To enable students to develop strong verbal communication skills, allowing them to collaborate effectively with team members, engage with stakeholders, and interact with the public, preparing them to excel as both team members and leaders.
4. To enable graduates to uphold professional ethics and fulfil their responsibilities in adherence to prevailing cyber laws.

5. To inculcate a sense of professional and social responsibility, encouraging graduates to actively contribute to society through involvement with professional organizations, educational institutions, civic groups, and community initiatives.

3. PROGRAMME OUTCOMES (POs):

PO1	Graduates get the ability to analyze and apply core principles of computing and mathematics relevant to the field of computer science and engineering.
PO2	Graduates will exhibit proficiency in understanding diverse computer programming languages and demonstrate knowledge of various technologies in computer systems.
PO3	Graduates will demonstrate an ability to apply mathematical foundations, algorithmic principles, and computer science theory, in the modelling and design of computer-based systems.
PO4	Graduates will demonstrate the ability to apply techniques and skills to analyze and investigate complex problems through research, effectively utilizing appropriate modern engineering tools to solve them.
PO5	Graduates will possess the ability to develop sustainable and inclusive technologies tailored to societal and environmental contexts.
PO6	Graduates will be able to communicate effectively while building self-confidence and embracing lifelong learning.
PO7	Graduates will exhibit leadership qualities, project management abilities, and financial expertise while upholding professional ethics.

4. PROGRAMME SPECIFIC OUTCOMES (PSO):

1. The graduates will demonstrate the ability to utilize advanced concepts in computer science to develop innovative solutions while fostering continuous learning and adaptability in emerging technologies.
2. The ability to solve complex engineering problems by applying advanced knowledge in data science, artificial intelligence, machine learning and cyber security grounded in the core principles and concepts of computer science.
3. The graduates will demonstrate the ability to leverage the fundamentals of computer science in competitive research and create innovative products that address societal needs, thereby emerging as a distinguished researcher and entrepreneur.

REGULATION

REGULATION FOR EXECUTIVE M. TECH IN COMPUTER SCIENCE AND ENGINEERING
UNDER OUTCOME BASED EDUCATION
&
CHOICE BASED CREDIT SYSTEM (CBCS) FRAMEWORK
(With Effect from the Academic Year 2025)

1. SCOPE:

These Regulations shall apply to the Executive MTech in Computer Science and Engineering program conducted by the Department of Computer Applications/Schools, Cochin University of Science and Technology.

The provisions herein supersede all other Regulations with respect to such PG programmes unless otherwise provided.

2. DEFINITIONS:

Department/School means Departments/Schools instituted in the University as per Statutes and Act.

Department Council (DC) The Department Council is a statutory body within each academic department. It typically includes all permanent faculty members of the department, with the Head of the Department serving as the chairperson. This council is responsible for making recommendations on the content of core and elective courses, including detailed syllabi for the programs offered by the department. These recommendations are submitted to the University and require approval from the relevant Board of Studies, Faculty, and the Academic Council. The Department Council also has the authority to design and introduce new elective or audited courses, modify or redesign existing electives, and replace current electives with new or revised ones to enhance student training and exposure.

Credit is the quantity of instruction given or the learning outcomes and a notional time to achieve those outcomes.

Core Course (CC) means a course that the student admitted to a particular programme must successfully complete in order to receive the Degree and which cannot be substituted by any other course. Core course is offered by the Department where the student takes admission.

Discipline Specific Elective (DSE) is a course of a particular discipline that a student has the choice to select from a pool of such courses from his/her programme of study. The DSEs to offer in a programme of study would be identified by the concerned Department/School.

Skill Enhancement Courses (SEC) are designed to develop Creativity, Critical Thinking, Communication, and Collaboration, which are known as 21st-century skills.

MOOC Course means a Massively Open Online Course offered by UGC, CUSAT or any other recognized educational agencies approved by the University.

3. ELIGIBILITY FOR ADMISSION:

B. Tech/B. E/AMIE degree in any discipline or MCA or MSc/MS degree in CS/IT/Electronics/Mathematics/Physics/Statistics or equivalent degree with a minimum of 50% or equivalent CGPA in the qualifying degree examination.

The candidates should be currently employed and have a minimum one year of working experience. Only the employment acquired after the award of the qualifying degree will be considered.

4. SANCTIONED INTAKE AND SELECTION CRITERIA:

The maximum intake of students in an academic year is 24. Statutory reservation of seats shall apply as per Government of Kerala rules.

The admission criteria for Executive M. Tech in Computer Science and Engineering programme is as follows:

GATE/DAT: Applicants will be ranked on the basis of their GATE score/ DAT (Department Admission Test) score conducted by the department concerned. In the absence of a valid GATE score, candidates will be considered for admission on the basis of score obtained in the DAT conducted by the Department concerned. However, preference for admission will be given to candidates with valid GATE score and financial Assistance through GATE Scholarship will not be provided to them.

Tie Breaking Criteria: In the case of admission to the Executive M. Tech program, wherever there is a tie in the GATE score/DAT score, the marks obtained in the qualifying examination will be considered as a tiebreaker. If the tie continues, date of birth (in descending order-older to younger) and name (in alphabetical order) will be considered in the respective order for breaking the tie.

5% Relaxation: Candidates with a valid GATE score in the concerned subject are eligible for 5% relaxation in the minimum mark requirement for qualifying examination, provided that the candidates have passed the qualifying examination.

5. STRUCTURE OF THE PROGRAM:

The Executive M. Tech in Computer Science and Engineering has a duration of 2 years, consisting of four semesters. The total credits for the course shall be 75. The credit distribution across the four semesters shall be 18, 19, 18, and 20 for semesters I, II, III, and IV respectively. An Executive M. Tech Degree in Computer Science and Engineering will be awarded to those who securing 75 credits and have satisfied the semester wise minimum credit distribution requirements as given:

6.

SEMESTER	CC	DSE	SEC	TOTAL
I	16	-	2	18
II	8	8	3	19
III	-	8	10	18
IV	-	-	20	20
				75

CREDIT DETAILS:

A course that includes one hour of lecture or tutorial or a minimum of two hours of lab work, practical work, or field work per week is given one credit.

One credit in a semester should be designed for 15 hours of Lectures or Tutorials or 30 hours of practicum and learner engagement in terms of course- related activities such as seminar preparation, submitting assignments, etc.

A one-credit seminar or internship or studio activities or field work/ projects or community engagement and service will have two-hour engagements per week (30 hours of engagement per semester).

7. COURSE REGISTRATION:

Every Department/School shall have Faculty Members as Student Advisors. Each student will be assigned to an Advisor/Mentor, by the Department council within one week from the commencement of the classes, who will counsel the student on the choice of elective courses depending on the student's academic background and objective. The student will then register for the courses he plans to take for the semester within the time prescribed by the University. The student should have completed the prescribed prerequisites if any for a course before registration. The Advisor/Mentor must keep all records of the candidate – attendance, internal marks, end semester marks etc.

Core courses of any programmes are to be compulsorily offered by the respective Department that offers the programme.

A student shall register and complete at least one Interdisciplinary/Industry based/Online course (MOOC) as one of the Electives before registering for the final semester of the Programme.

8. MODE OF DELIVERY OF CURRICULUM:

The curriculum delivery is designed in online mode, supplemented with offline lab sessions and MOOC components.

9. Massive Open Online Course (MOOC):

Students may be permitted to enrol in a credit-based MOOC course of minimum 12 weeks duration from SWAYAM/NPTEL/CUSAT or any other platforms approved by the Department Council. In the case of MOOC courses attended by the student, a certificate of satisfactory completion and marks/ grade if any issued by the authority who conducted the course must be submitted to the Head of the Department. The Department will conduct a viva on the subject of the online course if necessary. On the completion of this, the Department Council can award the respective weightage/grade to the student.

10. EVALUATION AND ELIGIBILITY FOR PASS:

A student would be considered to have progressed satisfactorily at the end of a semester if he/she has a minimum of 75 % attendance.

The evaluation scheme for each semester contains two parts, a Continuous Assessment (CA) and a Semester End Examination (SEE). The final result in each course will be determined on the basis of continuous assessment and performance in the end semester examination which will be in the ratio of 50:50 in the case of theory courses. For Laboratory Courses (Practical Courses) and Seminar there shall be only Continuous Assessment (CA) as per the procedures laid down by the Department Council.

Continuous Assessment (CA): The student shall be evaluated continuously throughout the semester and marks shall be awarded on the basis of tests / assignments as detailed below:

There shall be two class tests, assignments and an end semester examination. The first class test carries 20 marks and will be based on the portions of the syllabi covered till then. The second class test also carries 20 marks and will be based on the portions covered till then after the first class test. A maximum of 10 marks will be awarded for the assignments.

Marks obtained in the continuous assessment shall be directly communicated to the students and any grievances may be addressed to the teacher concerned or the Head of the Department (HOD) with supporting documents. The teacher and the HOD will examine the case and decide on his/her grievance. If the student is not convinced with the decision, he/she can approach the appellate authority, which is the department council, in writing and the council shall examine the same and take a final decision which has to be intimated to the student in writing. The decision of the appellate authority shall be final.

Semester End Examination (SEE):

The end semester examination will be for 50 marks and shall contain questions from the entire syllabus of the course. The duration of the end semester examination shall be three hours.

The question paper for the semester end examination shall be set by the concerned teacher in advance, which shall be scrutinized by the respective department council or by a committee consisting of the HOD and faculty members offering courses in that semester to ensure that questions are within the scope of the syllabus and that the entire syllabus of the course is fairly covered in the question paper. Modifications can be suggested by the council if necessary and such suggestions shall be incorporated in the final version of the question paper.

Students are required to physically appear for all examinations, including class tests, lab examination and the end-semester examination.

There shall be only a single evaluation for the semester end examination. Immediately after the end semester examination is over, the Head of the Department shall make arrangements to complete the evaluation and finalize the results within 10 working days.

The pass minimum in a subject is 50 %, with a separate minimum of 45% for end semester examination.

The final marks and grade in all the courses obtained by the students in that semester will be communicated to them directly. Those who could not obtain 50% marks (Grade D) in total for a course will be declared as failed in that course. Those who fail in any course shall approach the teacher concerned, if necessary, for a re-examination of the semester end examination. An additional semester-end examination for these candidates shall be conducted by the department within ten days of the result publication. This re-examination is only to provide the student a chance to pass the examination by completing the course successfully. If he/she completes the course successfully making use of this additional chance, he/she will be awarded only a D grade enabling the candidate to be declared successful in that course. If he/she cannot make it up, he/she may repeat the semester end examination of that course along with the subsequent batches, or re-register and repeat the course. In this case he/she will be awarded whatever grade he/she has secured.

All practical examinations will also be internally evaluated as per the procedures laid down by the Department Councils concerned.

Dissertation Evaluation: Dissertation evaluation shall be done at the end of III and IV semesters. The evaluation at the end of III and IV Semester shall be conducted by an examination committee consisting of the head of the department, a senior faculty member nominated by the head and the project guide. At the end of IV semester, the students will have to submit a dissertation on his / her project work to the Head of the Department within the last date prescribed for the purpose. The dissertation will be evaluated by an examination committee consisting of the head of the department, a senior faculty member or an external expert from another university or industry nominated by the HOD and the project guide. The candidate shall make an open

presentation of his/her dissertation which will be followed by a viva-voce examination. For the purpose of assessment, the performance of a student in the dissertation may be divided into the following sub components:

At the end of III semester:

(i) Assessment by the project guide (based on periodic assessment of the work of the candidate) - 50 %
(ii) Assessment by the examination committee - 50%

At the end of IV semester:

(i) Assessment by the project guide (based on periodic assessment of the work of the candidate) - 50 %
(ii) Assessment by the examination committee - 50%

11. **EVALUATION AND ELIGIBILITY FOR PASS:**

The result of all the examinations will be finalised and published by the department council, which will act as the passing board and the minutes shall be sent to the controller of examinations for issue of grade card. The University under its seal shall issue a Grade Card to the students on completion of each semester. The Grade card shall contain the following:

a.	Title of the course taken as core, elective and audit. (An audit course shall be listed only if the student has secured a pass)
b.	The credits associated with and the grades awarded for each course.
c.	The number of credits (core and elective separately) earned by the student and the Grade point Average.
d.	The total credits (core and elective) earned till that semester.

The following grades will be awarded based on the overall performance in each subject:

Range of Marks	Grades	Weightage
90 and above	S - Outstanding	10
80 to 89	A - Excellent	9
70 to 79	B - Very Good	8
60 to 69	C - Good	7
50 to 59	D - Satisfactory	6
Below 50	F - Failed	0

Overall performance at the end of the semester will be indicated by Grade Point Average (GPA) calculated as follows:

$$GPA = \frac{(G1C1+G2C2+G3C3+\ldots\ldots..GnCn)}{(C1+C2+C3+\ldots\ldots\ldots\ldots\ldots\ldots Cn)}$$

Where 'G' refers to the grade weightage and 'C' refers to the credit value of the corresponding course undergone by the student. At the end of the final semester Cumulative Grade Point Average (CGPA) will be calculated based on the above formula, considering the Credits and Grades earned during the entire programme of study. Classification for the Degree will be given as follows based on the CGPA:

(i) First Class with distinction 8 and above

(ii) First Class 6.5 and above

(iii) Second Class 6 and above

The Grade Card issued at the end of the final semester shall contain the details of all the courses taken which shall include the titles of the courses, the credits associated with each course, the CGPA and the class.

12. MONITORING AND MANAGEMENT OF PROGRAMMES:

Every post graduate programme conducted in the Departments shall be Monitored by the Department Council subject to these regulations. Such monitoring shall include design of programmes, prescribing the mode of conduct of the programmes and monitoring the evaluation process of students.

13. ACADEMIC COMMITTEE:

There shall be an Academic Committee constituted by the Vice-Chancellor to monitor and co-ordinate the working of the CBCS System.

The Committee shall consist of:

The Pro-Vice-Chancellor Chairman

The Registrar Secretary

The Controller of Examinations

One Teacher from each Department

A Senior Professor nominated by the Vice-Chancellor from among the members of the Committee shall be the Vice-Chairman of the Committee.

The term of the office of the committee shall be two years, but the committee once constituted shall continue in office until a reconstituted committee assumes office.

14. TRANSITORY PROVISION:

Notwithstanding anything contained in these regulations, the Vice-Chancellor shall, for a period of one year from the date of coming into force of these regulations, have the power to provide by order that these regulations shall be applied to any programme with such modifications as may be necessary.

COURSE STRUCTURE
(APPENDIX I)

1. CREDIT SCHEME:

The total credits for the course shall be 75. The credit distribution across the four semesters shall be 18, 19, 18, and 20 for semesters I, II, III, and IV respectively.

Semester	Credits
Semester I	18
Semester II	19
Semester III	18
Semester IV	20
Total	**75**

2. PROGRAM STRUCTURE:

2.1 Course Category and Definition

Course Category	Definition
CC	**Core Course**
EC	**Elective Course**
SEC	**Skill Enhancement Course**

2.2 Course Category-wise Credit Distribution

Sl. No	Course Category	No. of Courses	Total Credits
1	Core Course	6	24
3	Elective Course	6	16
4	Skill Enhancement Course	5	35

2.3 Course Structure

Executive M. Tech in Computer Science and Engineering spreads over four semester as under:

SEMESTER I

Course Code	Name of the course	CC/ EC/ SEC	Credit	Marks		Total Marks
				CE	SEE	
CC101	Linear Algebra and Probability Theory	CC	4	50	50	100
CC102	Advanced Data Structures and Algorithms	CC	4	50	50	100
CC103	Advanced Machine Learning Techniques	CC	4	50	50	100
CC104	Secure Software Development	CC	4	50	50	100
SEC101	Software Design and Development Lab	SEC	2	50	-	50

SEMESTER II

Course Code	Name of the course	CC/ EC/ SEC	Credit	Marks		Total Marks
				CE	SEE	
CC201	Quantum Computing	CC	4	50	50	100
CC202	Research Methodology	CC	4	50	50	100
EC201	Professional Elective - I	EC	3	50	50	100
EC202	Professional Elective - II	EC	3	50	50	100
EC203	Professional Elective - III (MOOC)	EC	2	-	100	100
SEC201	Seminar	SEC	1	50	-	50
SEC202	Data Science Lab/AI and ML Lab/Cybersecurity Lab	SEC	2	50	-	50

SEMESTER III

Course Code	Name of the course	CC/ EC/ SEC	Credit	Marks		Total Marks
				CE	SEE	
EC301	Professional Elective - IV	EC	3	50	50	100
EC302	Professional Elective - V (MOOC)	EC	2	50	50	100
EC303	Professional Elective - VI	EC	3	50	50	100
SEC301	Dissertation Phase - I	SEC	10	50	50	100

SEMESTER IV

Course Code	Name of the course	CC/ EC/ SEC	Credit	Marks		Total Marks
				CE	SEE	
SEC401	Dissertation Phase - I and Viva Voce	SEC	20	50	50	100

Elective Courses:

1. **AI and Machine Learning**
   - EC201 - Deep Learning
   - EC202 - Computer Vision and Image Processing
   - EC203 - MOOC
   - EC301 - Reinforcement Learning
   - EC302 - MOOC
   - EC303 - Explainable AI and Model Interpretability
2. **Data Science**
   - EC201 - Deep Learning
   - EC202 - Data Visualization and Predictive Analytics
   - EC203 - MOOC
   - EC301 - Scalable Machine Learning for Big Data
   - EC302 - MOOC
   - EC303 - Explainable AI and Model Interpretability
3. **Cyber Security**
   - EC201 - Cloud Security and Privacy
   - EC202 - Blockchain and Decentralized Security
   - EC203 - MOOC
   - EC301 - Cyber Forensics
   - EC302 - MOOC
   - EC303 - Artificial Intelligence for Cyber Security

13. Massive Open Online Course (MOOC)

Students may be permitted to enrol in a credit-based MOOC course of minimum 12 weeks duration from SWAYAM/NPTEL/CUSAT or any other platforms approved by the Department Council. In the case of MOOC courses attended by the student, a certificate of satisfactory completion and marks/ grade if any issued by the authority who conducted the course must be submitted to the Head of the Department. The Department will conduct a viva on the subject of the online course if necessary. On the completion of this, the Department Council can award the respective weightage/grade to the student.

SYLLABUS
(APPENDIX II)

SEMESTER 1

CC101 Linear Algebra and Probability Theory

Course Outcomes:

After the completion of this course, the students shall be able to:

CO1	Solve systems of linear equations and analyze matrix operations, subspaces, and orthogonal projections.	(Cognitive Level:Apply)
CO2	Apply eigenvalues, diagonalization, and singular value decomposition in linear transformations and data analysis.	(Cognitive Level:Apply)
CO3	Model and analyze data using probability distributions and hypothesis testing.	(Cognitive Level:Apply)
CO4	Interpret random variables, their distributions, and processes, including Markov processes and the Central Limit Theorem.	(Cognitive Level:Apply)

Mapping of course outcomes with program outcomes- **Low = 1, Medium =2, High =3**

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PSO1**	**PSO2**	**PSO3**
CO1	**2**	**2**						**1**		
CO2	**3**	**3**		**2**				**3**	**2**	
CO3	**3**		**3**			**3**		**3**		
CO4	**3**							**2**	**1**	

Unit I

Systems of linear equations, Row reduction and echelon forms, Matrix operations, including inverses, Block matrices, Linear dependence and independence, Subspaces and bases and dimensions, Orthogonal bases and orthogonal projections.

Unit II

Gram-Schmidt process, Linear models and least-squares problems, Determinants and their properties, Cramer's Rule, Eigenvalues and eigenvectors, Diagonalization of a matrix, Symmetric matrices, Positive definite matrices, Similar matrices, Linear transformations, Singular Value Decomposition.

Unit III

Basics of probability, joint, marginal and conditional probability, Bayes theorem examples of calculating probability, Discrete probability distributions – Binomial, Poisson, and multinomial distributions. Continuous probability distributions – Normal, exponential and chi-square, problems related to discrete and continuous probability distributions, testing of hypothesis.

Unit IV

Random variables (discrete and continuous), and their distributions Covariance - Correlation and Linear regression - Transformation of random variables. i. i. d random variables and Central limit theorem. Definition of a random process, stationarity, Markov Process.

Text Books/References

1. Gilbert Strang, "Linear Algebra and Its Applications", Fourth Edition, Cengage, 2006
2. Poole, Linear Algebra: A Modern Introduction, 2nd Edition, Brooks/Cole, 2005.
3. Howard Anton and Chris Rorrs, "Elementary Linear Algebra", Ninth Edition, John Wiley & Sons, 2000.
4. Douglas C. Montgomery and George C. Runger, "Applied Statistics and Probability for Engineers", Third Edition, John Wiley and Sons Inc., 2003.
5. Ronald E. Walpole, "Probability and Statistics for Engineers and Scientists", Seventh Edition, Pearson Education, Asia, 2002.

CC102 Advanced Data Structures and Algorithms

Course Outcomes:

After the completion of this course, the students shall be able to:

CO1	Analyze algorithm efficiency using growth functions, recurrences, probability distributions, and basic data structures.	(Cognitive Level:Analyze)
CO2	Implement and evaluate balanced trees, disjoint set structures, and fundamental graph algorithms for real-world applications.	(Cognitive Level:Apply)
CO3	Apply advanced sorting techniques, graph algorithms, and algorithmic paradigms like greedy, dynamic programming, and backtracking.	(Cognitive Level:Apply)
CO4	Understand computational complexity classes, NP-	(Cognitive

	completeness, approximation algorithms, and randomized algorithms for solving intractable problems.	Level:Understand)

Mapping of course outcomes with program outcomes- **Low = 1, Medium =2, High =3**

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PSO1	PSO2	PSO3
CO1	**2**	**2**						**1**		
CO2	**3**	**3**						**3**	**2**	
CO3	**3**		**2**	**2**				**3**	**2**	
CO4	**3**		**3**	**3**				**2**	**3**	

Unit I

Review of order rotation & growth of functions, recurrences, probability distributions, Average case analysis of algorithms, Basic data structures such as stacks, queues, linked lists, and applications. Direct access tables and hash tables, hash functions and relates analysis, Binary Search trees and Operations.

Unit II

Balancing operations in AVL Trees and Red-Black Trees, B-Trees – definition – properties, operations, data structures for disjoint sets, Graph algorithms, MST single source all pair shortest paths, BFS, DFS, topological sort, strongly connected components.

Unit III

Quicksort randomized version, searching in linear time, More graph algorithms – maximal independent sets, coloring vertex cover, introduction to perfect graphs. Algorithmic paradigms Greedy Strategy, Dynamic programming, Backtracking, Branch-and-Bound.

Unit IV

Tractable and Intractable Problems, Complexity Classes – P, NP, NP- Hard and NP-Complete Classes- NP Completeness proof of Clique Problem and Vertex Cover Problem-Approximation algorithms- Bin Packing, Graph Coloring. Randomized Algorithms (Definitions of Monte Carlo and Las Vegas algorithms), Randomized version of Quick Sort algorithm with analysis

Text Books/References

1. T.H.Cormen, C.E.Leiserson, R.L.Rivest, C. Stein, Introduction to Algorithms, 2nd Edition, Prentice-Hall India (2001)
2. Ellis Horowitz, Sartaj Sahni, Sanguthevar Rajasekaran, "Fundamentals of ComputerAlgorithms", 2nd Edition, Orient Longman Universities Press (2008)
3. Sara Baase and Allen Van Gelder —Computer Algorithms, Introduction to Design andAnalysis, 3rd Edition, Pearson Education (2009)

CC103 Advanced Machine Learning Techniques

Course Outcomes:

After the completion of this course, the students shall be able to:

CO1	Distinguish between traditional and machine learning approaches, understand types of machine learning, and build predictive and classification models using supervised learning techniques.	(Cognitive Level:Apply)
CO2	Apply unsupervised learning methods, including clustering and dimensionality reduction techniques, to analyze and interpret data.	(Cognitive Level:Apply)
CO3	Understand reinforcement learning concepts, algorithms, and applications, including Q-Learning and SARSA.	(Cognitive Level:Understand)
CO4	Develop the ability to model complex systems using probabilistic graphical models.	(Cognitive Level:Apply)

Mapping of course outcomes with program outcomes- **Low = 1, Medium =2, High =3**

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PSO1**	**PSO2**	**PSO3**
CO1	**2**	**3**						**1**		**1**
CO2	**3**	**2**	**2**					**3**	**2**	
CO3	**3**	**2**	**3**					**3**	**2**	
CO4	**3**							**2**	**3**	

Unit I

Traditional Learning vs Machine Learning – Various types of Machine Learning: Supervised Learning – Unsupervised Learning – Reinforcement Learning – Machine Learning workflow – Machine Learning issues and challenges. Predictive Models: Regression – Multivariate Regression – Types of Regression Models – Estimation of Regression coefficients – issues and challenges – applications. – Classification Models: Introduction – Different types of classifiers: Perceptron – Naive Bayes – Decision Tree – Logistic Regression – K-Nearest Neighbor – Artificial Neural Networks – Support Vector Machine – Evaluation metrics for supervised learning.

Unit II

Unsupervised Learning - Clustering Models: Partitioning based clustering – Hierarchical based clustering – Density based clustering – Grid based clustering – Mixture Models and EM Algorithm – Fuzzy k-Means Algorithm – Evolution metrics for clustering models - Dimensional Reduction Techniques: Need – Various types: PCA – ICA – FA – t-SNE - Case studies.

Unit III

Reinforcement Learning – Introduction to Reinforcement Learning – Learning Task – Example of Reinforcement Learning in Practice – Learning Models for Reinforcement – Markov Decision process – Q Learning – Q Learning function – Q Learning Algorithm – SARSA algorithm – Nondeterministic Rewards and Actions – Applications of Reinforcement Learning.

Unit IV

Probabilistic Graphical Models: Bayesian networks, Markov Networks, Factor Graph Representation, HMMs, CRFs, Exponential Family. Exact Inference: Variable Elimination, Junction Tree Algorithm. Belief Propagation (Loopy or not). Sampling Based Approximate Inference: MCMC, Metropolis Hastings, Gibbs Sampling.

Text Books/References

1. Ethem Alpaydin, Introduction to Machine Learning, 4th edition, MIT Press 2020.
2. Bishop, Christopher M., Pattern Recognition and Machine Learning. Springer-Verlag, 2006.
3. Zhi-Hua Zhou, Ensemble Methods: Foundations and Algorithms, CRC Press, 2012.
4. Lior Rokach, Ensemble Learning: Pattern Classification using Ensemble Methods, 2nd ed., World Scientific, 2019.
5. Tom M. Mitchell, Machine Learning, McGraw-Hill Education (India) Private Limited, 2013
6. Stephen Marsland, Machine Learning: An Algorithmic Perspective, CRC Press, 2014.

7. Andrew Glassner, Deep Learning from basics to practice. Volume1 & 2, Kindle Edition, 2018.
8. Koller, D. and Friedman, N. (2009). Probabilistic Graphical Models: Principles and Techniques. MIT Press.

CC104 Secure Software Development

Course Outcomes:

After the completion of this course, the students shall be able to:

CO1	Understand fundamental security concepts, attack types, malware, and vulnerabilities to analyze and mitigate security risks.	(Cognitive Level:Understand)
CO2	Apply secure software development practices throughout the Software Development Life Cycle (S-SDLC) and implement threat identification and risk mitigation techniques.	(Cognitive Level:Apply)
CO3	Protect against various attacks, such as DoS, buffer overflows, and insecure coding issues, using countermeasures and secure coding practices in C and Java.	(Cognitive Level:Apply)
CO4	Address vulnerabilities like SQL injection, XSS attacks, and race conditions while designing secure applications and developing effective security testing plans.	(Cognitive Level:Apply)

Mapping of course outcomes with program outcomes- **Low = 1, Medium =2, High =3**

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PSO1**	**PSO2**	**PSO3**
CO1	**2**		**1**		**1**			**1**	**2**	
CO2	**3**	**2**	**2**		**1**		**1**	**3**	**1**	
CO3	**3**	**2**	**2**				**1**	**3**	**2**	

CO4	**3**	**3**	**3**					**2**		

Unit I

Security, CIA Triad, Viruses, Trojans, and Worms In a Nutshell, Security Concepts- exploit, threat, vulnerability, risk, attack. Malware Terminology: Rootkits, Trapdoors, Botnets, Key loggers, Honeypots. Active and Passive Security Attacks. IP Spoofing, Tear drop, DoS, DDoS,XSS, SQL injection, Smurf, Man in middle, Format String attack. Types of Security Vulnerabilities- buffer overflows, Invalidated input, race conditions, access-control problems, weaknesses in authentication, authorization, or cryptographic practices. Access Control Problems.

Unit II

Proactive Security development process, Secure Software Development Cycle (S-SDLC) , Security issues while writing SRS, Design phase security, Development Phase, Test Phase, Maintenance Phase, Writing Secure Code – Best Practices SD3 (Secure by design, default and deployment), Security principles and Secure Product Development Timeline. Identifying the Threats by Using Attack Trees and rating threats using DREAD, Risk Mitigation Techniques and Security Best Practices. Security techniques, authentication, authorization. Defence in Depth and Principle of Least Privilege.

Unit III

Protection against DoS attacks, Application Failure Attacks, CPU Starvation Attacks, Insecure Coding Practices In Java Technology. ARP Spoofing and its countermeasures. Buffer Overrun- Stack overrun, Heap Overrun, Array Indexing Errors,Format String Bugs. Security Issues in C Language: String Handling, Avoiding Integer Overflows and Underflows and Type Conversion Issues- Memory Management Issues, Code Injection Attacks, Canary based countermeasures using StackGuard and Propolice. Socket Security, Avoiding Server Hijacking, Securing RPC, ActiveX and DCOM.

Unit IV

SQL Injection Techniques and Remedies,Race conditions, Time of Check Versus Time of Use and its protection mechanisms. Validating Input and Interprocess Communication, Securing Signal Handlers and File Operations. XSS scripting attack and its types – Persistent and Non persistent attack XSS Countermeasures and Bypassing the XSS Filters. Security code overview, secure software installation. The Role of the Security Tester, Building the Security Test Plan. Testing HTTP-Based Applications, Testing File-Based Applications, Testing Clients with Rogue Servers.

Text Books/References

1. Writing Secure Code, Michael Howard and David LeBlanc,Microsoft Press, 2nd Edition, 2004.
2. Buffer Overflow Attacks: Detect, Exploit, Prevent by Jason Deckard ,Syngress,1st Edition, 2005.
3. Threat Modeling, Frank Swiderski and Window Snyder,Microsoft Professional, 1st Edition ,2004.

SEC101 Software Design and Development Lab

Course Outcomes:

After the completion of this course, the students shall be able to:

CO1	Develop and implement advanced data structures like AVL trees and Red-Black trees, and apply graph traversal techniques like BFS and DFS for solving computational problems.	(Cognitive Level:Apply)
CO2	Apply algorithms such as Dijkstra's and Bellman-Ford for shortest path detection and Kruskal's and Prim's for constructing minimum spanning trees in graph-based scenarios.	(Cognitive Level:Apply)
CO3	Solve optimization problems using dynamic programming techniques and demonstrate secure coding practices to mitigate vulnerabilities like SQL injection, buffer overflows, and cross-site scripting.	(Cognitive Level:Apply)
CO4	Design and simulate secure authentication protocols, including multi-factor authentication systems, to ensure robust security in software applications.	(Cognitive Level:Apply)

Mapping of course outcomes with program outcomes- **Low = 1, Medium =2, High =3**

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PSO1**	**PSO2**	**PSO3**
CO1	**2**		**3**		**1**			**1**	**2**	
CO2	**3**	**2**	**1**	**2**	**1**			**3**	**3**	

CO3	**2**	**3**		**2**	**1**			**3**	**2**	
CO4	**2**	**1**	**1**					**2**		

List of Experiments:

1. Develop AVL trees, Red-Black Trees for specific use cases and Perform insertion, deletion, and search operations.
2. Apply breadth-first search (BFS) and depth-first search (DFS) to solve problems like connected components and topological sorting.
3. Implement Dijkstra's algorithm and Bellman-Ford algorithm for shortest path detection
4. Apply Kruskal's and Prim's algorithms for minimum spanning tree construction.
5. Solve problems like the knapsack problem, matrix chain multiplication, and longest common subsequence using dynamic programming techniques.
6. Detect and fix vulnerabilities like SQL injection, buffer overflows, and cross-site scripting in sample web applications.
7. Write programs to demonstrate secure coding practices, including input validation, data sanitization, and error handling.
8. Simulate authentication protocols such as Kerberos or design a simple multi-factor authentication system.

Semester -II

CC201 - Quantum Computing

Course Outcomes:

After the completion of this course, the students shall be able to:

CO1	Understand foundational concepts in quantum mechanics, quantum computation, and key quantum algorithms, including superdense coding and Bell inequalities.	(Cognitive Level:Understand)
CO2	Develop quantum circuits using single, two-qubit, and universal gates, and apply quantum algorithms like quantum search and Fourier transform to computational problems.	(Cognitive Level:Apply)
CO3	Explore the physical realization of quantum computers, quantum noise, quantum operations, and their applications in solving computational challenges.	(Cognitive Level:Apply)
CO4	Analyze quantum error-correction techniques, stabilizer codes, and fault-tolerant quantum computation to ensure resilient quantum information processing.	(Cognitive Level:Analyze)

Mapping of course outcomes with program outcomes- **Low = 1, Medium =2, High =3**

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PSO1	PSO2	PSO3
CO1	**3**		**1**		**1**			**1**		
CO2	**1**	**2**	**2**		**1**			**3**	**2**	
CO3	**2**	**2**	**3**		**2**			**3**	**1**	
CO4	**2**	**3**						**2**		

Unit I

Review of Linear Algebra: Vector Space, Hilbert Space, Bases, Matrices, Eigenvalues and Eigenvectors, Hermitian matrices, and Unitary matrices. Introduction to Quantum Computing. Dirac Notation, Qubits, Bloch Sphere, Postulates of Quantum Mechanics, Classical Computation Vs Quantum Computation. Quantum algorithms summarized - Quantum information - Postulates of quantum mechanics - Application: superdense coding - Density operator - Schmidt decomposition and purifications - EPR and the Bell inequality.

Unit II

Measurements: Composite system, reduced state, mixed state. Single Qubit gates – two-qubit gates – Multiple Qubits gates, Universal gates, Quantum circuit model of computation, Quantum computational complexity - no-cloning theorem. Applications: order-finding and factoring - General applications of the quantum Fourier - Quantum search algorithms - Quantum search as a quantum simulation, Quantum counting - Speeding up the solution of NP-complete problems.

Unit III

Quantum computers: physical realization - Guiding principles - Conditions for quantum computation- Harmonic oscillator quantum computer - Quantum information - Quantum noise and quantum operations - Classical noise and Markov processes, Quantum operations Examples of quantum noise and quantum operations - Applications of quantum operations - Limitations of the quantum operations formalism.

Unit IV

Distance measures for quantum information - Distance measures for classical information- the closeness of two quantum states –Quantum error-correction- Three qubit bit flip code - Shor code, Theory of quantum error-correction- Constructing quantum codes - Classical linear codes - Stabilizer codes - Stabilizer formalism - Fault-tolerance: the big picture- Fault-

tolerant quantum logic- Fault-tolerant measurement- Elements of resilient quantum computation.

Text Books/ References

1. Nielsen, M., & Chuang, I. In Quantum Computation and Quantum Information: 10th Anniversary Edition, Cambridge: Cambridge University Press, 2010.
2. Rieffel, Eleanor G., and Wolfgang H. Polak. "Quantum computing: A gentle introduction (scientific and engineering computation)." The MIT Press 10 (2014): 1973124.
3. John Gribbin, Computing with Quantum Cats: From Colossus to Qubits, Prometheus Books, 2014.
4. B.N. Murdin Quantum Computing from the Ground Up, by Riley Tipton Perry, Contemporary Physics, 2013.
5. Tannor, David J. Introduction to quantum mechanics: a time-dependent perspective. 2007.

CC202 Research Methodology

Course Outcomes:

After the completion of this course, the students shall be able to:

CO1	Understand the objectives, types, and methodologies of research, and design appropriate research frameworks for social and physical sciences.	(Cognitive Level:Understand)
CO2	Collect, process, and analyze primary and secondary data using various sampling techniques and ensure validity and reliability in data collection.	(Cognitive Level:Apply)
CO3	Apply statistical methods for hypothesis testing, correlation, regression, and advanced analyses like ANOVA, factor analysis, and clustering to derive meaningful insights.	(Cognitive Level:Apply)
CO4	Conduct literature reviews, interpret research findings, and prepare structured research reports with proper citations and bibliographies.	(Cognitive Level:Apply)

Mapping of course outcomes with program outcomes- **Low = 1, Medium =2, High =3**

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PSO1	PSO2	PSO3
CO1	**3**	**3**						**1**	**3**	**1**
CO2	**2**	**2**	**2**		**1**			**3**	**2**	
CO3	**2**	**1**	**1**		**1**			**3**	**2**	
CO4	**3**	**1**	**1**					**2**		

Unit 1

Meaning, objectives and significance of research, types and parameters of research, research process, identification and definition of the research problem, definition of construct and variables, pure and applied research design, exploratory and descriptive design methodology, qualitative vs. quantitative research methodology, field studies, field experiments vs. laboratory experiments, research design in social and physical sciences.

Unit II

Survey, assessment and analysis: data collection, primary and secondary sources of data, Collection of primary data through questionnaire and schedules. Collection of secondary data, processing and analysis of data. Sample survey, simple random sampling, stratified random sampling, systematic sampling, cluster sampling, area sampling and multistage sampling. Pilot survey, scaling techniques, validity & reliability.

Unit III

Procedure for testing of hypothesis, the null hypothesis, determining levels of significance, type i and ii errors, grouped data distribution, measures of central tendency, measures of spread/dispersion, normal distribution, analysis of variance: one way, two way, chi square test and its application, students 'T' distribution, non-parametric statistical techniques, binomial test. Correlation and regression analysis – discriminate analysis – factor analysis – cluster analysis, measures of relationship.

Unit IV

Review of literature: historical survey and its necessity, layout of research plan, meaning, techniques and precautions of interpretation, types of report: technical report, popular report, report writing – layout of research report, mechanics of writing a research report. Writing bibliography and references.

Text Books/References

1. Research in education, By J W Best and J V Kahn, Pearson/ Allyn and Bacon.
2. Research Methodology – Methods and Techniques, C K Kothari, New Age International.
3. Design and Analysis of Experiments, D C Montgomery, Wiley.
4. Applied Statistics & Probability for Engineers, D C Montgomery & G C Runger, Wiley.
5. Management Research Methodology: Integration of Principles, Methods and Techniques, K N Krishnaswamy, A I Sivakumar and M Mathiranjan, Pearson Education.

EC201 - Professional Elective - I - Deep Learning

Course Outcomes:

After the completion of this course, the students shall be able to:

CO1	Compare the computational Performance of Parallel Computation on CPUs and GPUs.	(Cognitive Level:Apply)
CO2	Examine the working of different types of Autoencoders and Generative Adversarial Networks.	(Cognitive Level:Apply)
CO3	Employ various RNN cell variants.	(Cognitive Level:Apply)
CO4	Describe the basic concepts in Reinforcement Learning and Unsupervised learning.	(Cognitive Level:Apply)

Mapping of course outcomes with program outcomes- **Low = 1, Medium =2, High =3**

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PSO1**	**PSO2**	**PSO3**
CO1	**2**	**3**						**1**	**3**	
CO2	**3**	**1**	**2**		**1**			**3**	**3**	**1**
CO3	**1**	**2**	**1**		**1**			**3**	**2**	**1**
CO4	**3**	**2**						**2**		

Unit 1

Introduction to Neural Networks: Perceptron, Multi-layer perceptron, Regularization, Hyperparameter tuning, GPUs, TPUs. Regression: Linear Regression, Multiple linear regression, Multivariate linear regression, Logistic regression.

Unit II

Convolution Neural Networks: Convolution operations, DCNN, VGG16 Advanced Convolution Neural Networks: AlexNet, Residual networks, DenseNets, Xception.

Unit III

Autoencoders: Introduction, Vanilla autoencoders, Sparse encoders, Denoising autoencoders, Stacked autoencoders, Variational Autoencoders. Generative Adversarial Networks: DCGAN, SRGAN, Cycle GAN, Info GAN. Recurrent Neural Network: RNN cell, RNN cell variants, RNN variants, RNN topologies.

Unit IV

EncoderDecoder architecture, Attention mechanism, Transformer architecture. Unsupervised Learning: Principal Component analysis, Self-organizing maps, Restricted Boltzmann Machines. Reinforcement Learning: Deep reinforcement learning agents,Deep Q-Networks, Deep deterministic policy gradient.

Text Books/ References

1. Deep learning with Tensor flow 2 and Keras,AntonioGulli,Amita Kapoor, Sujith Pal,2019
2. Dive into Deep Learning, Aston Zhang, Zachary C. Lipton, Mu Li, and Alexander J. Smola,2020
3. Deep Learning, Ian Goodfellow and YoshuaBengio and Aaron Courville, MIT Press, 2016.
4. Yuxi(Hayden), Liu and Savansh Mehta, “Hands -on Deep Learning Architectures with Python”, Packt, 2019.
5. Josh Patterson & Adam Gibson, “Deep Learning: A Practitioners Approach”, published by O’Reilly Media.,2017
6. Nikhil Ketkar, “Deep Learning with Python”, published by Apress Media,2017

EC201 - Professional Elective - I - Cloud Security and Privacy

Course Outcomes:

After the completion of this course, the students shall be able to:

CO1	Understand the basic components of cloud & Security in the cloud.	(Cognitive Level:Understand)
CO2	Illustrate the Infrastructure Security, Data Security, storage and security management in the cloud.	(Cognitive Level:Apply)
CO3	Understand the concepts of Identity and Access Management.	(Cognitive Level:Understand)
CO4	Illustrate the privacy issues in cloud environments.	(Cognitive Level:Apply)

Mapping of course outcomes with program outcomes- **Low = 1, Medium =2, High =3**

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PSO1**	**PSO2**	**PSO3**
CO1	**1**	**1**						**3**	**2**	**1**
CO2	**3**	**3**	**2**	**1**	**1**			**2**	**3**	**1**
CO3	**3**	**3**	**2**	**2**	**1**			**1**	**1**	
CO4	**2**	**2**	**1**		**1**			**3**	**1**	

Unit I

Cloud Computing: The SPI Framework for Cloud Computing, Relevant Technologies in Cloud Computing, The Traditional Software Model,The Cloud Services Delivery Model, Cloud Deployment Models, Key Drivers to Adopting the Cloud, The Impact of Cloud Computing on Users, Governance in the Cloud, Barriers to Cloud Computing Adoption in the Enterprise. Infrastructure Security: Infrastructure Security: The Network Level, Infrastructure Security: The Host Level, Infrastructure Security: The Application Level.

Unit II

Data Security and Storage: Aspects of Data Security, Data Security Mitigation, Provider Data and Its Security. Identity and Access Management: Trust Boundaries and IAM, Why IAM?,IAM Challenges, IAM Definitions, IAM Architecture and Practice, Getting Ready for the Cloud, Relevant IAM Standards and Protocols for Cloud Services, IAM Practices in the Cloud, Cloud Authorization Management, Cloud Service Provider IAM Practice

Unit III

Security Management in the Cloud: Security Management Standards, Security Management in the Cloud Availability Management, SaaS Availability Management PaaS Availability Management, IaaS Availability Management, Access Control, Security Vulnerability, Patch, and Configuration Management

Unit IV

Privacy, Data Life Cycle, Key Privacy Concerns in the Cloud, Who Is Responsible for Protecting Privacy, Changes to Privacy Risk Management and Compliance in Relation to Cloud Computing, Legal and Regulatory Implications, U.S. Laws and Regulations, International Laws and Regulations.

Text Books/References

1. Tim Mather, Subra Kumara swamy,Shahed Latif,"Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance" O'ReillyMedia; 1st edition [ISBN:0596802765], 2009 .
2. RonaldL.Krutz,RussellDeanVines,"CloudSecurity"[ISBN:0470589876],2010.
3. John Rittinghouse, James Ransome, "Cloud Computing" CRC Press; 1 edition [ISBN:1439806802],2009.
4. J.R.("Vic")Winkler,"SecuringtheCloud"Syngress[ISBN:1597495921]2011 1stEdition,KindleEdition

EC202 - Professional Elective - II - Data Visualization and Predictive Analytics

Course Outcomes:

After the completion of this course, the students shall be able to:

CO1	Understand data acquisition processes, cleaning, transformation, and visualization techniques to analyze complex datasets effectively.	(Cognitive Level:Understand)
CO2	Utilize data visualization tools for rank, trend, multivariate, distribution, correlation, and geographical analysis, including interactive visualizations.	(Cognitive Level:Apply)

CO3	Apply regression model-building frameworks, including simple linear regression, to analyze relationships between variables and validate models.	(Cognitive Level:Apply)
CO4	Develop multiple linear regression models, addressing challenges like heteroscedasticity, multicollinearity, outliers, and variable transformation for robust analysis.	(Cognitive Level:Apply)

Mapping of course outcomes with program outcomes- **Low = 1, Medium =2, High =3**

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PSO1**	**PSO2**	**PSO3**
CO1	**2**	**3**		**2**				**1**	**3**	
CO2	**1**	**3**	**2**	**1**	**1**			**3**	**3**	**1**
CO3	**2**	**2**	**2**		**1**			**3**	**1**	
CO4	**3**	**1**		**1**				**2**	**2**	

Unit I

Introduction to Data Acquisition – Applications –Process- Data Extraction- Data Cleaning and Annotation- Data Integration -Data Reduction- Data Transformation –Visualization- Introduction Terminology- Basic Charts and Plots- Multivariate Data Visualization- Data Visualization Techniques– Pixel-Oriented Visualization Techniques- Geometric Projection Visualization Techniques- Icon-Based Visualization Techniques- Hierarchical Visualization Techniques- Visualizing Complex Data and Relations.

Unit II

Data Visualization Tools– Rank Analysis Tools- Trend Analysis Tools- Multivariate Analysis Tools- Distribution Analysis Tools- Correlation Analysis Tools- Geographical Analysis Tools. Interactive visualization.

Unit III

Regression model building framework: Problem definition, Data pre-processing; Model building; Diagnostics and validation Simple Linear Regression: Coefficient of determination, Significance tests, Residual analysis, Confidence and Prediction intervals.

Unit IV

Multiple Linear Regression: Coefficient of multiple coefficient of determination, Interpretation of regression coefficients, Categorical variables, Heteroscedasticity, Multi-collinearity, outliers, Auto regression and transformation of variables, Regression model building.

Text Books/References

1. Andy Kirk, Data Visualization A Handbook for Data Driven Design, Sage Publications, 2016.
2. Philipp K. Janert, Gnuplot in Action, Understanding Data with Graphs, Manning Publications, 2010.
3. Alberto Cordoba, "Understanding the Predictive Analytics Lifecycle", Wiley, 2014.
4. Eric Siegel, Thomas H. Davenport, "Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die", Wiley, 2013.
5. James R Evans, "Business Analytics – Methods, Models and Decisions", Pearson 2013.

EC202 - Professional Elective - II - Computer Vision and Image Processing

Course Outcomes:

After the completion of this course, the students shall be able to:

CO1	Compare Feature detection and image transformation techniques.	(Cognitive Level:Apply)
CO2	Apply segmentation and Feature-based alignment.	(Cognitive Level:Apply)
CO3	Apply structure from motion and perform dense motion estimation.	(Cognitive Level:Apply)
CO4	Apply depth estimation, Object Detection, Face recognition, Instance recognition and understand multi-camera views.	(Cognitive Level:Apply)

Mapping of course outcomes with program outcomes- **Low = 1, Medium =2, High =3**

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PSO1**	**PSO2**	**PSO3**
CO1	**1**	**2**			**1**			**2**	**3**	

CO2	**3**	**3**	**2**	**1**	**1**			**3**	**2**	
CO3	**3**	**3**	**2**	**1**				**3**	**1**	
CO4	**2**	**3**	**1**					**3**	**3**	

Unit I

Digital Image Formation and Representation: Fundamentals of Image Formation, Geometric Primitives and Transformations: Orthogonal, Euclidean, Affine, Projective; Photometric Image 96 Formation, Digital Camera, Low-level Image processing: Fourier Transform, Convolution and Filtering, Image Enhancement, Restoration, Histogram Processing.

Unit II

Feature Detection: Edges - Canny, Laplacian of Gaussian (LoG), Difference of Gaussian (DoG); Lines - Hough Transform, Corners - Harris and Hessian Affine, Orientation Histogram, SIFT, SURF, HOG, GLOH, Scale-Space Analysis- Image Pyramids and Gaussian derivative filters Gabor Filters and DWT. Image Segmentation: Region Growing, Edge Based approaches to segmentation, Graph-Cut, Mean-Shift, Markov Random Field Segmentation, Texture Segmentation; Feature-based Alignment: 2D and 3D Feature-based alignment, Pose estimation, Geometric intrinsic calibration.

Unit III

Structure from motion: Triangulation, Two-frame structure from motion, Factorization, Bundle adjustment, constrained structure and motion; Dense motion estimation – Translational alignment, Parametric motion, Spline-based motion, Optical flow, Layered motion.

Unit IV

Depth estimation and Multi-camera views: Perspective, Binocular Stereopsis: Camera and Epipolar Geometry; Homography, Rectification, 3-D reconstruction framework; Autocalibration. Stereo; Recognition - Object Detection, Face recognition, Instance recognition.

Text Books/References

1. Richard Szeliski, Computer Vision: Algorithms and Applications, Springer-Verlag London Limited 2011.
2. Computer Vision: A Modern Approach, D. A. Forsyth, J. Ponce, Pearson Education, 2003.
3. Richard Hartley and Andrew Zisserman, Multiple View Geometry in Computer Vision, Second Edition, Cambridge University Press, March 2004.

4. K. Fukunaga; Introduction to Statistical Pattern Recognition, Second Edition, Academic Press, Morgan Kaufmann, 1990.
5. R.C. Gonzalez and R.E. Woods, Digital Image Processing, Addison- Wesley, 1992.
6. Christopher M. Bishop; Pattern Recognition and Machine Learning, Springer, 2006

EC202 - Professional Elective - II - Blockchain and Decentralized Security

Course Outcomes:

After the completion of this course, the students shall be able to:

CO1	Use the working of an immutable distributed ledger and trust model that defines blockchain.	(Cognitive Level:Apply)
CO2	Illustrate the essential components of a blockchain platform.	(Cognitive Level:Apply)
CO3	Understand the security perspective of blockchain technology.	(Cognitive Level:Understand)
CO4	Learn and apply security analysis and performance-enhancing techniques related to blockchain.	(Cognitive Level:Apply)

Mapping of course outcomes with program outcomes- **Low = 1, Medium =2, High =3**

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PSO1**	**PSO2**	**PSO3**
CO1	**3**	**1**		**1**				**2**		
CO2	**1**	**3**	**1**	**1**				**3**	**2**	**1**
CO3	**2**	**3**	**1**					**3**	**2**	**2**
CO4	**1**	**2**	**3**	**1**				**3**		

Unit I

Distributed Database, Two General Problem, Byzantine General Problem and Fault Tolerance, Hadoop Distributed File System, Distributed Hash Table, ASIC resistance, Turing Complete. Cryptography: Hash function, Digital Signature - ECDSA, Memory Hard Algorithm, and Zero Knowledge Proof.

Unit II

Advantage over conventional distributed database, Blockchain Network, Mining Mechanism, Distributed Consensus, Merkle Patricia Tree, Gas Limit, Transactions and Fee, Anonymity, Reward, Chain Policy, Life of Blockchain application, Soft & Hard Fork, Private and Public blockchain. Nakamoto consensus, Proof of Work, Proof of Stake, Proof of Burn, Difficulty Level, Sybil Attack, Energy utilization and alternate.

Unit III

Blockchain Related Issues, Higher-Level Language (Solidity) RelatedIssues, EVM Bytecode Related Issues, Real-Life Attacks on Blockchain Applications/Smart Contracts, Trusted Execution Environments. Security Tools for Smart Contracts- Working, Advantages, And Disadvantages ofTools- Oyente, Securify, Maian, Manticore, Mythril, SmartCheck, Verx. Secure KeyManagement, Quantum Resilience Keys.

Unit IV

Performance related Issues- Transaction Speed, Transaction Fees, Network Size,Complexity, Interoperability Problems, Lack of Standardization. Lack of SupportiveRegulations Related to Blockchain Applications. Off-Chain State Channels, Sidechains, Parallels Chains,Concurrent Smart Contract Transactions, Sharding Technique and Its Benefits, AtomicSwaps Between Smart Contracts.

Text Books/References

1. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, 2016
2. Kumar Saurabh, AshutoshSaxena, Blockchain Technology: Concepts and Applications, Wiley, 2020 .
3.Mastering Ethereum: Building Smart Contracts and Dapps Book by AndreasAntonopoulos and Gavin Wood, Shroff Publisher/O′Reilly Publisher, 2018.
4. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder, "BitcoinandCryptocurrency Technologies: A Comprehensive Introduction", Princeton University Press, July, 2016.
5. SachinShetty, Charles A. Kamhoua, Laurent L. Njilla, Blockchain for Distributed Systems Security, Wiely, 2019
6. Rahul Neware Dr. Brajesh Kumar, Er. ParagRastogi ,Dr. HarshalPatil, BLOCKCHAIN SECURITY, Book Rivers; 1st edition, 2022

7.YassineMaleh , Mohammad Shojafar , MamounAlazab , ImedRomdhani,Blockchain For Cybersecurity And Privacy: Architectures Challenges And Applications, Taylor & Francis Ltd, 2020
8. Corresponding Online Resources: https://www.edx.org/course/blockchain-andfintech-basics-applications-and-limitations

EX202- Data Science Lab/AI and ML Lab/Cybersecurity Lab

Data Science Lab:

Experiment 1: Download, install and explore the features of NumPy, SciPy, Jupyter, Statsmodels and Pandas packages.
Experiment 2: Working with Numpy arrays.
Experiment 3: Working with Pandas data frames
Experiment 4: Reading data from text files, Excel and the web and exploring various commands for doing descriptive analytics on the Iris data set
Experiment 5:

1. Univariate analysis: Frequency, Mean, Median, Mode, Variance, Standard Deviation, Skewness and Kurtosis.
2. Bivariate analysis: Linear and logistic regression modeling
3. Multiple Regression analysis.
4. Compare the results of the above analysis for the two data sets

Experiment 6:

1. Normal curves
2. Density and contour plots.
3. Correlation and scatter plots
4. Histograms
5. Three dimensional plotting

Experiment 7: Visualizing Geographic Data with Basemap

AI and ML Lab:

Experiment 1: Introduction to Python for Data Science and ML
Experiment 2: Data Preprocessing and Feature Engineering
Experiment 3: Implementing Linear Regression
Experiment 4: Logistic Regression for Classification
Experiment 5: K-Nearest Neighbors (K-NN) Classification
Experiment 6: Support Vector Machines (SVM) for Classification
Experiment 7: Decision Trees and Random Forests
Experiment 8: K-Means Clustering
Experiment 9: Naive Bayes Classification
Experiment 10: Neural Networks and Deep Learning

Cybersecurity Lab:

Experiment 1: Introduction to Cybersecurity Tools and Environment Setup
Experiment 2: Network Scanning and Enumeration with Nmap
Experiment 3: Wireshark Packet Sniffing and Analysis
Experiment 4: Vulnerability Scanning with OpenVAS
Experiment 5: Password Cracking with Hashcat
Experiment 6: Ethical Hacking: Exploiting Vulnerabilities with Metasploit
Experiment 7: SQL Injection Attacks and Mitigation
Experiment 8: Man-in-the-Middle (MITM) Attack with SSL Stripping

EC301 - Professional Elective - IV - Scalable Machine Learning for Big Data

Course Outcomes:

After the completion of this course, the students shall be able to:

CO1	Understand the challenges of machine learning for big data and explore distributed computing frameworks and data pipelines for scalable solutions.	(Cognitive Level:Understand)
CO2	Develop scalable supervised and unsupervised learning models, including regression, classification, clustering, and dimensionality reduction, to handle large-scale datasets.	(Cognitive Level:Apply)
CO3	Apply advanced techniques such as distributed deep learning, federated learning, and real-time analytics for big data processing.	(Cognitive Level:Apply)
CO4	Explore practical applications of scalable machine learning in domains like healthcare, e-commerce, and social media, leveraging tools and frameworks.	(Cognitive Level:Apply)

Mapping of course outcomes with program outcomes- **Low = 1, Medium =2, High =3**

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PSO1**	**PSO2**	**PSO3**
CO1	**3**	**1**						**2**		
CO2	**3**	**3**	**1**	**1**				**3**	**2**	**1**

CO3	**3**	**3**	**2**	**1**				**3**	**2**	**1**
CO4	**2**	**2**		**1**				**3**	**2**	

Unit I

Challenges in machine learning for big data, Distributed computing frameworks including Hadoop, Apache Spark, and MapReduce, Data pipelines and workflows for big data, Feature engineering for large datasets, Case study on scaling machine learning workflows.

Unit II

Parallel and distributed algorithms for regression and classification, Scalable versions of linear regression, logistic regression, and support vector machines (SVM), Distributed gradient descent and optimization techniques, Scalable tree-based methods including Random Forests and Gradient Boosted Trees, Evaluation and validation techniques for large-scale datasets.

Unit III

Distributed clustering algorithms including scalable k-Means, DBSCAN, and Spectral Clustering, Matrix factorization techniques for large-scale data such as Singular Value Decomposition (SVD) and Principal Component Analysis (PCA), Graph-based learning at scale including community detection and label propagation, Case study on clustering in large-scale social network data.

Unit IV

Deep learning for big data including distributed training of neural networks, model parallelism, and data parallelism, Introduction to federated learning and its applications, Real-time machine learning with streaming data using frameworks like Spark Streaming and Kafka, Scalable recommendation systems including collaborative filtering and matrix factorization, Applications of scalable machine learning in healthcare, e-commerce, and social media.

Text Books / References

1. Jimmy Lin and Chris Dyer, *Data-Intensive Text Processing with MapReduce*, Morgan & Claypool Publishers, 2010.
2. Jure Leskovec, Anand Rajaraman, and Jeffrey Ullman, Mining of Massive Datasets, Cambridge University Press, 2020.
3. Trevor Hastie, Robert Tibshirani, and Jerome Friedman, The Elements of Statistical Learning: Data Mining, Inference, and Prediction, Springer, 2009.
4. Benjamin Bengfort, Rebecca Bilbro, and Tony Ojeda, Applied Text Analysis with Python: Enabling Language-Aware Data Products with Machine Learning, O'Reilly Media, 2018.

EC301 - Professional Elective - IV - REINFORCEMENT LEARNING

Course Outcomes:

After the completion of this course, the students shall be able to:

CO1	Understand foundational probability concepts and Markov Decision Processes (MDPs), including Bellman equations, to model and analyze decision-making problems.	(Cognitive Level:Understand)
CO2	Apply dynamic programming techniques, such as policy iteration and value iteration, to solve prediction and control problems in MDPs with theoretical proofs of convergence.	(Cognitive Level:Apply)
CO3	Implement Monte Carlo and Temporal Difference (TD) methods for model-free reinforcement learning, including SARSA and Q-learning, for effective prediction and control.	(Cognitive Level:Apply)
CO4	Explore function approximation techniques, including gradient-based methods and deep Q-networks, to address complex reinforcement learning problems with large state-action spaces.	(Cognitive Level:Apply)

Mapping of course outcomes with program outcomes- **Low = 1, Medium =2, High =3**

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PSO1**	**PSO2**	**PSO3**
CO1	**1**	**2**						**1**		
CO2	**3**	**3**	**2**	**1**				**3**	**2**	**1**
CO3	**3**	**3**	**2**	**1**				**3**	**2**	**1**
CO4	**2**	**3**						**2**		

Unit I

Probability Primer: Brush up of Probability concepts - Axioms of probability, concepts of random variables, PMF, PDFs, CDFs, Expectation. Concepts of joint and multiple random

variables, joint, conditional and marginal distributions. Correlation and independence. Markov Decision Process: Introduction to RL terminology, Markov property, Markov chains, Markov reward process (MRP). Introduction to and proof of Bellman equations for MRPs along with proof of existence of solution to Bellman equations in MRP. Introduction to Markov decision process (MDP), state and action value functions, Bellman expectation equations, optimality of value functions and policies, Bellman optimality equations.

Unit II

Prediction and Control by Dynamic Programming: Overview of dynamic programming for MDP, definition and formulation of planning in MDPs, principle of optimality, iterative policy evaluation, policy iteration, value iteration, Banach fixed point theorem, proof of contraction mapping property of Bellman expectation and optimality operators, proof of convergence of policy evaluation and value iteration algorithms, DP extensions.

Unit III

Monte Carlo Methods for Model Free Prediction and Control: Overview of Monte Carlo methods for model free RL, First visit and every visit Monte Carlo, Monte Carlo control, On policy and off policy learning, Importance sampling. TD Methods: Incremental Monte Carlo Methods for Model Free Prediction, Overview TD(0), TD(1) and TD(λ), k-step estimators, unified view of DP, MC and TD evaluation methods, TD Control methods - SARSA, Q-Learning and their variants.

Unit IV

Function Approximation Methods: Getting started with the function approximation methods, Revisiting risk minimization, gradient descent from Machine Learning, Gradient MC and Semi-gradient TD(0) algorithms, Eligibility trace for function approximation, Afterstates, Control with function approximation, Least squares, Experience replay in deep Q-Networks.

Text Books/References

1. Reinforcement Learning: An Introduction", Richard S. Sutton and Andrew G. Barto, 2nd Edition.
2. Machine Learning: A Probabilistic Perspective", Kevin P. Murphy.
3. Probability, Statistics, and Random Processes for Electrical Engineering", 3rd Edition, Alberto Leon-Garcia.

Web Resources

1. https://nptel.ac.in/courses/106106143
2. https://www.coursera.org/specializations/reinforcement-learning

EC301 - Professional Elective - IV - CYBER FORENSICS

Course Outcomes:

After the completion of this course, the students shall be able to:

CO1	Explain systematic approach to computer investigations.	(Cognitive Level:Apply)
CO2	Apply forensic procedure to collect and recover digital evidence using tools.	(Cognitive Level:Apply)
CO3	Judge the validity of digital evidence before presenting using cryptographic hashes and Create forensic duplicates for investigation using tools and commands for capturing digital evidence	(Cognitive Level:Apply)
CO4	Describe steps to follow for network, email and mobile forensics.	(Cognitive Level:Apply)

Mapping of course outcomes with program outcomes- **Low = 1, Medium =2, High =3**

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PSO1**	**PSO2**	**PSO3**
CO1	**2**	**1**						**1**	**2**	
CO2	**3**	**3**	**2**					**3**	**3**	**1**
CO3	**3**	**3**	**2**					**3**	**3**	**1**
CO4	**3**	**2**						**2**	**3**	

Unit I

Computer Forensics Fundamentals: Computer Crime, challenges with computer crime, different types of computer crime-Identity Theft, Identity fraud, Email and internet Fraud, Theft of financial data, Corporate Data Theft, Cyber extortion-Ransomware attack, Phishing, Hacking, Spoofing, Harassment, Intellectual property Theft, Ethical Hacking, Windows Hacking . Computer Forensics Fundamentals- Type of Computer Forensics Technology, Computer forensics specialist approaches - Scientific method in forensic analysis, Computer Forensics Services.

Unit II

Computer Forensics Evidence and Capture, Data Recovery-Evidence collection - archiving , artifacts , systematic collections steps, controlling contamination , reconstructing the attacks . Data Seizure - Duplication and preservation of Digital Evidence, Computer image verification and Authentication-Cryptographic Hashes. Data Acquisition. Investigating Cybercrime, Duties Support Functions and Competencies.

Unit III

Types of Evidence: The Rules of Evidence, Volatile Evidence, order of volatility- Why Collect Evidence in the first place, Collection Options Obstacles. Computer forensics and network forensics, systematic procedure for network forensics analysis. Incident - Incident Response Methodology - Steps, Activities in Initial Response Phase after detection of an incident, Creating response toolkit. Initial Response & Volatile Data Collection from Windows system - Initial Response & Volatile Data Collection from Unix system, Forensic Duplication, Qualified Duplication, Forensic Duplicates as Admissible Evidence, Forensic Duplication using Linux commands, creating windows Forensic Duplicate using tool, Forensic Duplicate of a Hard Disc.

Unit IV

Collecting Network-Based Evidence - Investigating Routers - Network Protocols - Email Tracing - Internet Fraud. Hackers Tools. Cell phone and mobile device forensics. Forensics hardware and software, Information Security Investigations, Corporate Cyber Forensics, investigating large scale Data breach cases, Analyzing Malicious software.

Text Books/References

1. Computer Forensics: Computer Crime Scene Investigation, John Vacca, Edition 1, 2015, Laxmi Publications.
2. A Practical Guide to Computer Forensics Investigation, Darren Hayes, 2014, Edition 1, Pearson IT Certification.
3. Hacking Exposed Computer Forensics, Aaron Philipp, Chris Davis, and David Cowen, Edition 2, 2009, McGraw Hill.
4. Insider Computer Fraud: An In-depth Framework for Detecting and Defending Against Insider IT Attacks, Kenneth Brancik, Edition 1, 2019, Auerbach Publications.
5. Guide to Computer Forensics and Investigations, Bill Nelson, Amelia Phillips, Christopher Steuart, Edition 6, 2020, Cengage Learning India Pvt. Ltd.
6. Cyber Forensics, Dejey, Murugan, Edition 1, 2018, Oxford University Press.

EC303 - Professional Elective - VI - Explainable AI and Model Interpretability

Course Outcomes:

After the completion of this course, the students shall be able to:

CO1	Analyse Global and local explanations using SHAP and LIME.	(Cognitive Level:Analyze)
CO2	Develop interpretable CNN, use unsupervised learning to perform exploratory analysis on a model.	(Cognitive Level:Apply)

CO3	Analyse counterfactual, contrastive XAI and interpret methods for multivariate forecasting and sensitivity analysis.	(Cognitive Level:Analyze)
CO4	Evaluate adversarial (evasion and poisoning) attacks on machine learning models.	(Cognitive Level:Apply)

Mapping of course outcomes with program outcomes- **Low = 1, Medium =2, High =3**

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PSO1**	**PSO2**	**PSO3**
CO1	**2**	**2**	**2**				**1**	**1**		
CO2	**3**	**3**	**2**	**1**	**1**	**1**		**3**	**2**	**1**
CO3	**3**	**3**	**2**	**1**		**1**		**3**	**3**	**1**
CO4	**3**	**2**	**1**			**1**		**2**	**2**	

Unit I

Machine Learning and Explainable AI, Need for XAI, Explainability and Interpretability, XAI Flow, Making ML Models Explainable: Intrinsic Explanations, Post Hoc Explanations, Global or Local Explainability, Properties of Explanations. Intrinsic Explainable Models: Loss Function, Linear Regression, Logistic Regression, Decision Trees, KNN. Model Agnostic Methods For XAI: Global Explanations, Local Explanations, Shap. Kernel Explainer, Local Linear Surrogate Models (LIME): Mathematical Representation, creating agnostic AutoML template, Bagging Classifier, Boosting Classifier, Decision Tree, Extra Trees, Creating Lime Explainer, SHAP for Boosted Trees.

Unit II

Explaining Deep Learning Models: Agnostic Approach - Adversarial Features, Augmentations, Occlusions as Augmentations, Occlusion as an Agnostic XAI Method. Opening Deep Networks: Layer Explanation, CAM and Grad-CAM, Deep Shap/ DeepLift. A critic of saliency method - Explainability Batch Normalisation Layer by Layer, Unsupervised methods.

Unit III

Counterfactual Explanations Method: Visualising Data Point using What - If-Tool, Exploring data points, The logic of counterfactual explanations, Contrastive Explanations Method (CEM), CEM Applied to example dataset using CNN, Autoencoders, Interpretation Methods for Multivariate Forecasting and Sensitivity Analysis: Accessing Time Series, odels with traditional interpretation, Generating LSTM attribution with integrated gradients, Compute Local and Global Attribution.

Unit IV

Understanding the Effect of Irrelevant Features, Feature Engineering, Detecting and Mitigating Bias, Adversarial Attacks, Evasion Attacks, defending against targeted attacks with preprocessing, Shielding against evasion attacks via adversarial training, Evaluating and certifying adversarial robustness.

Text Books/Reference Books

1. Explainable AI with Python, Leonida Gianfagna, Antonio Di Cecco, Edition 2, 2021, Springer.
2. Hands-On Explainable AI (XAI) with Python: Interpret, visualize, explain, and integrate reliable AI for fair, secure, and trustworthy AI apps, by Denis Rothman, Edition 1, 2020, Packt Publishing Limited.
3. Interpretable Machine Learning", by Christoph Molnar, Edition 2, 2020, Lulu.com.
4. Interpretable Machine Learning with Python: Learn to build interpretable high-performance models with hands-on real-world examples", by Serg Masís, Edition 1, 2021, Packt Publishing Limited.

EC303 - Professional Elective - VI - Artificial Intelligence for Cyber Security

Course Outcomes:

After the completion of this course, the students shall be able to:

CO1	Understand the role of AI in cyber defense and its application in detecting and mitigating evolving cyber threats.	(Cognitive Level:Understand)
CO2	Develop skills to apply machine learning and deep learning methods for intrusion detection and vulnerability analysis.	(Cognitive Level:Apply)
CO3	Understand adversarial AI attacks and implement ethical and transparent defense mechanisms.	(Cognitive Level:Understand)
CO4	Explore AI-driven solutions for securing emerging technologies, including IoT, cloud, and blockchain systems.	(Cognitive Level:Apply)

Mapping of course outcomes with program outcomes- **Low = 1, Medium =2, High =3**

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PSO1	PSO2	PSO3
CO1	2	1		1	1		1	1	2	
CO2	3	3	2	2	1	1	2	3	3	1
CO3	3	3	2	1			1	3	3	
CO4	3	2		1				2	3	

Unit I

Role of artificial intelligence in cyber defense, Machine learning for threat detection and response, Supervised and unsupervised learning for anomaly detection, AI-based malware detection, Case study: AI-driven phishing detection systems.

Unit II

AI-powered intrusion detection systems (IDS), Deep learning for zero-day vulnerability detection, Natural language processing (NLP) for analyzing phishing emails and social engineering threats, Case study: AI for advanced persistent threat (APT) detection.

Unit III

Adversarial attacks on machine learning models, Defense strategies against adversarial threats, Ethical challenges in deploying AI in cyber defense, Ensuring fairness and transparency in AI-driven security systems, Case study: Mitigating adversarial attacks on spam filters.

Unit IV

AI in IoT and cloud security, Predictive analytics for blockchain and smart contract security, Autonomous threat hunting with reinforcement learning, AI-driven cyber forensics and evidence analysis, Case study: Securing critical infrastructure using AI.

Text Books / References

1. Alessandro Parisi,Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies, Packt Publication, 2019
2. Gupta, Brij B., and Quan Z. Sheng, eds. Machine learning for computer and cyber security: principle, algorithms, and practices. CRC Press, 2019.
3. Artificial Intelligence and Data Mining Approaches in Security Frameworks Editor(s):Neeraj Bhargava, Ritu Bhargava, Pramod Singh Rathore, Rashmi Agrawal, 2021.
4. Clarence Chio and David Freeman (2018). Machine Learning and Security: Protecting Systems with Data and Algorithms O'REILLY Publications.
5. McKinney, W Brij B. Gupta and Quan Z. Sheng.(2019). Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices (Cyber Ecosystem and Security), CRC Press Publication.

****