COURSE STRUCTURE & SYLLABUS

FOR

MASTER OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

BATCH 2025 AND ONWARDS

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
ISLAMIC UNIVERSITY OF SCIENCE AND TECHNOLOGY, KASHMIR

MTech CSE Semester-Wise Credit Distribution

S. No.	Semester	Credits
01	I	18
02	II	16
03	III	16
04	IV	16
Total Credits		**66**

Semester–I

S. No.	Course Code	Course Title	L-T-P	Credits
1.	CSE501C	Mathematical Foundations of Computer Science	3-0-0	3
2.	CSE502C	Advanced Network Security	3-0-0	3
3.	CSE503C	Machine Learning	3-0-0	3
4.	CSE504C	Cyber Physical Systems	3-0-0	3
5.	CSE505C	Research Methodology	3-0-0	3
6.	CSE506C	Advanced Network Security Lab	0-0-2	1
7.	CSE507C	Machine Learning Lab	0-0-2	1
8.	CSE508C	Cyber Physical Systems Lab	0-0-2	1
Total				**18**

Semester–II

S. No.	Course Code	Course Title	L-T-P	Credits
1.	CSE550C	Advanced Computer Architecture	3-0-0	3
2.	CSE551C	Advanced Data Structures and Algorithms	3-0-0	3
3.		Elective-I	3-0-2	4
4.		Elective-II	3-0-0	3
5.	CSE552C	Data Analytics using Python	0-0-2	1
6.	CSE553C	Advanced Data Structures and Algorithms Lab	0-0-2	1
7.	CSE554C	Seminar	0-0-0	1
Total				**16**

Semester–III

S. No.	Course Code	Course Title	L-T-P	Credits
1.		Elective-III	3-0-2	4
2.		Elective-IV	3-0-0	3
3.		Elective-V	3-0-0	3
4.	CSE601C	Project-I	0-0-12	6
Total				**16**

Semester–IV

S. No.	Course Code	Course Title	L-T-P	Credits
1.	CSE650C	Project-II	0-0-32	16
Total				**16**

PROFESSIONAL ELECTIVE COURSES: VERTICALS

VERTICAL I: CYBER SECURITY

S. No.	Course Code	Course Title	L-T-P	Credits
1.	CSE550E	Python for Cybersecurity	3-0-2	4
2.	CSE551E	Wireless and Mobile Security	3-0-2	4
3.	CSE552E	Network Forensics and Intrusion Detection	3-0-2	4
4.	CSE553E	Cybersecurity Attack and Defense Fundamentals	3-0-2	4
5.	CSE566E	Applied Cryptography	3-0-0	3
6.	CSE567E	Secure Systems Architecture and Design	3-0-0	3
7.	CSE568E	Quantum Cryptography and Information Security	3-0-0	3
8.	CSE569E	Cyber Threat Intelligence	3-0-0	3
9.	CSE601E	Penetration Testing, Incident Response and Forensics	3-0-2	4
10.	CSE602E	Cybersecurity for Internet of Things	3-0-2	4
11.	CSE603E	Blockchain Security	3-0-2	4
12.	CSE604E	Machine Learning for Cybersecurity	3-0-2	4
13.	CSE617E	Cloud Security	3-0-0	3
14.	CSE618E	Cybersecurity for Mobile and Web applications	3-0-0	3
15.	CSE619E	Cybersecurity Risk Management Framework	3-0-0	3
16.	CSE620E	Network Security and Database Vulnerabilities	3-0-0	3

VERTICAL II: INTERNET OF THINGS

S. No.	Course Code	Course Title	L-T-P	Credits
1.	CSE554E	Embedded System Design	3-0-2	4
2.	CSE555E	Microcontrollers for IoT prototyping	3-0-2	4
3.	CSE556E	Data Acquisition	3-0-2	4
4.	CSE557E	IoT Programming and Big Data	3-0-2	4
5.	CSE570E	Principles of Sensors and Signal Conditioning	3-0-0	3
6.	CSE571E	Architecting Smart IoT Devices	3-0-0	3
7.	CSE572E	IoT Communications and Networks	3-0-0	3
8.	CSE573E	Software Architecture for IoT	3-0-0	3
9.	CSE605E	Cloud Computing for IoT	3-0-2	4
10.	CSE606E	Programming Internet of Things	3-0-2	4
11.	CSE607E	Artificial Intelligence of Things	3-0-2	4
12.	CSE608E	IoT Applications and Web Development	3-0-2	4
13.	CSE621E	IoT Security and Trust	3-0-0	3
14.	CSE622E	IoT Data Analytics	3-0-0	3
15.	CSE623E	Advanced IoT Systems Integration and Industrial Applications	3-0-0	3
16.	CSE624E	Software Defined Networks with IoT	3-0-0	3

VERTICAL III: ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

S. No.	Course Code	Course Title	L-T-P	Credits
1.	CSE558E	Deep Learning	3-0-2	4
2.	CSE559E	Data Warehousing and Data Mining	3-0-2	4
3.	CSE560E	Natural Language Processing	3-0-2	4
4.	CSE561E	Distributed Machine Learning	3-0-2	4
5.	CSE574E	Soft Computing	3-0-0	3
6.	CSE575E	Cloud Computing for Machine Learning	3-0-0	3
7.	CSE576E	Bioinformatics and Computational Biology	3-0-0	3
8.	CSE577E	Optimization Techniques for Machine Learning	3-0-0	3
9.	CSE609E	Machine Learning for IoT	3-0-2	4
10.	CSE610E	Computer Vision	3-0-2	4
11.	CSE611E	Data Visualization	3-0-2	4
12.	CSE612E	Natural Computing Algorithms	3-0-2	4
13.	CSE625E	Statistical Methods in Decision Making	3-0-0	3
14.	CSE626E	AI in Cyber Security	3-0-0	3
15.	CSE627E	Generative Adversarial Network	3-0-0	3
16.	CSE628E	Quantum Machine Learning	3-0-0	3

VERTICAL IV: GENERAL

S. No.	Course Code	Course Title	L-T-P	Credits
1.	CSE562E	Advanced Database Systems	3-0-2	4
2.	CSE563E	Semantic Web Technologies	3-0-2	4
3.	CSE564E	Back End Development Technologies	3-0-2	4
4.	CSE565E	High Performance Computing Systems	3-0-2	4
5.	CSE578E	Graph Theory	3-0-0	3
6.	CSE579E	Human Computer Interaction	3-0-0	3
7.	CSE580E	Modern Operating Systems	3-0-0	3
8.	CSE581E	Architecting Social Networks	3-0-0	3
9.	CSE613E	Front End Development Technologies	3-0-2	4
10.	CSE614E	Social Network Analysis and Mining	3-0-2	4
11.	CSE615E	Social Network Security and Analysis	3-0-2	4
12.	CSE616E	Health Informatics	3-0-2	4
13.	CSE629E	Application Development	3-0-0	3
14.	CSE630E	Advanced IoT Systems Integration and Industrial Applications	3-0-0	3
15.	CSE631E	Optimization Methods	3-0-0	3
16.	CSE632E	Algorithmic Game Theory	3-0-0	3

Elective-I

S. No.	Cyber Security	Internet of Things	Artificial Intelligence and Machine Learning	General Electives
1.	Python for Cybersecurity	Embedded System Design	Deep Learning	Advanced Database Systems
2.	Wireless and Mobile Security	Microcontrollers for IoT prototyping	Data Warehousing and Data Mining	Semantic Web Technologies
3.	Network Forensics and Intrusion Detection	Data Acquisition	Natural Language Processing	Back End Development Technologies
4.	Cybersecurity Attack and Defense Fundamentals	IoT Programming and Big Data	Distributed Machine Learning	High Performance Computing Systems

Elective-II

S. No.	Cyber Security	Internet of Things	Artificial Intelligence and Machine Learning	General Electives
1.	Applied Cryptography	Principles of Sensors and Signal Conditioning	Soft Computing	Graph Theory
2.	Secure Systems Architecture and Design	Architecting Smart IoT Devices	Cloud Computing for Machine Learning	Human Computer Interaction
3.	Quantum Cryptography and Information Security	IoT Communications and Networks	Bioinformatics and Computational Biology	Modern Operating Systems
4.	Cyber Threat Intelligence	Software Architecture for IoT	Optimization Techniques for Machine Learning	Architecting Social Networks

Elective-III

S. No.	Cyber Security	Internet of Things	Artificial Intelligence and Machine Learning	General Electives
1.	Penetration Testing, Incident Response and Forensics	Cloud Computing for IoT	Machine Learning for IoT	Front End Development Technologies
2.	Cybersecurity for Internet of Things	Programming Internet of Things	Computer Vision	Social Network Analysis and Mining
3.	Blockchain Security	Artificial Intelligence of Things	Data Visualization	Social Network Security and Analysis
4.	Machine Learning for Cybersecurity	Software Defined Networks with IoT	Natural Computing Algorithms	Health Informatics

Elective-IV

S. No.	Cyber Security	Internet of Things	Artificial Intelligence and Machine Learning	General Electives
1.	Cloud Security	IoT Security and Trust	Statistical Methods in Decision Making	Application Development
2.	Cybersecurity for Mobile and Web applications	IoT Data Analytics	AI in Cyber Security	Advanced IoT Systems Integration and Industrial Applications
3.	Cybersecurity Risk Management Framework	Advanced IoT Systems Integration and Industrial Applications	Generative Adversarial Network	Optimization Methods
4.	Network Security and Database Vulnerabilities	IoT Applications and Web Development	Quantum Machine Learning	Algorithmic Game Theory

ELECTIVE-V

S. No.	Course Code	Course Title	L-T-P	Credits
1.	CSE633E	Business Analytics	3-0-0	3
2.	CSE634E	Software Project Planning and Management	3-0-0	3
3.	CSE635E	Operations Research	3-0-0	3
4.	CSE636E	Information and Communication Technology Policy and Regulation	3-0-0	3
5.	CSE637E	Simulation and Modelling	3-0-0	3

DETAILED SYLLABUS

SEMESTER I

Course Code: **CSE501C**	**Mathematical Foundations of Computer Science**	Credits: **03** L T P 3 0 0

Course Outcomes

- Solve computational problems using propositional/predicate logic and number theory (congruences, Fermat's theorem, Chinese remainder theorem).
- Apply algebraic structures (groups, rings, fields) and linear algebra (vector spaces, eigenvalues) to computer science problems.
- Analyze discrete/continuous random variables and probability distributions using counting and inequalities (Markov's, Chebyshev's).
- Design algorithms for graph problems using Euler tours, planarity, coloring, and max-flow min-cut theorem.
- Evaluate computational complexity using Turing machines, NP-hard/complete classes, and approximation algorithms.

Unit I
Functional Logic: Proposition Logic, Resolution Proof system, Predicate logic. Congruences, Fermat's theorem, Euler function, Chinese remainder theorem.

Unit II
Groups, homomorphism theorems, cosets and normal subgroups, Lagrange's theorem, Ring. Field. Linear algebra: Vector Space, Basis, Matrices and Linear Transformations, Eigen values, Orthogonality.

Unit III
Counting, Probability, Discrete random variable, Continuous random variable, Moment generating function, Markov's inequality, Chebyshev's inequality, The geometric and binomial distributions, The tail of the binomial distribution.

Unit IV
Graphs, Euler tours, planar graphs, Hamiltonian graphs, Euler's formula, applications of Kuratowski's theorem, graph colouring, chromatic polynomials, trees, weighted trees, the max-flow min-cut theorem.

Unit V
Turing Machines, Recursive and Recursively Enumerable languages. Cantor's Diagonalization theorem. Complexity classes NP-Hard and NP-complete Problems Cook's theorem NP completeness reductions. Approximation algorithms.

Books
1. Donald F. Stanat and David F. McAllister, Discrete mathematics in Computer Science.
2. Thomas Koshy, Elementary number theory with Applications, Elsevier
3. I.N. Herstein, Topics in Algebra. John Wiley & Sons.
4. Sheldon M. Ross, Introduction to Probability Models, Elsevier.
5. H. Cormen, C. E. Leiserson, R. L. Rivest, C Stein, Introduction to Algorithms, Prentice Hall India.
6. Sara Baase and Alan Van Van Gelder. Computer Algorithms: Introduction to Design and Analysis. Addison – Wiley, 2000.
7. G. Chartrand and P. Zhang, Introduction to Graph Theory, McGraw-Hill Companies,
8. Douglas B. West, Introduction to Graph Theory, Prentice Hall of India.
9. Linear Algebra 2nd Edition (Paperback) by Kenneth Hoffman, Ray Kunze, PHI Learning, 2009.
10. Discrete Mathematics and Its Applications by Kenneth H. Rosen
11. Abstract Algebra: An Introduction" by Thomas W. Hungerford
12. Linear Algebra and Its Applications by Gilbert Strang
13. Introduction to the Theory of Computation by Michael Sipser
14. Introduction to Graph Theory by Douglas B. West

Course Code: **CSE502C**	**Advanced Network Security**	Credits: **03** L T P 3 0 0

Course Outcomes
- Classify the encryption techniques.
- Illustrate the key management technique and authentication.
- Evaluate the security techniques applied to network and transport layer
- Discuss the application layer security standards.
- Apply security practices for real time applications.

Unit I
Basics of cryptography, conventional and public-key cryptography, hash functions, authentication, and digital signatures.

Unit II
Key Management and Distribution: Symmetric Key Distribution, Distribution of Public Keys, X.509 Certificates, Public-Key Infrastructure. User Authentication: Remote User-Authentication Principles, Remote User-Authentication Using Symmetric Encryption, Kerberos Systems, Remote User Authentication Using Asymmetric Encryption.

Unit III
Network Access Control: Network Access Control, Extensible Authentication Protocol, IEEE 802.1X, Port-Based Network Access Control IP Security Internet Key Exchange (IKE). Transport-Level, Security: Web Security Considerations, Secure Sockets Layer, Transport Layer Security, HTTPS, standard, Secure Shell (SSH) application.

Unit IV
Electronic Mail Security: Pretty Good Privacy, S/MIME, Domain Keys Identified Mail. Wireless Network Security: Mobile Device Security

Unit V
Firewalls and Intrusion Detection Systems: Intrusion Detection Password Management, Firewall Characteristics Types of Firewalls, Firewall Basing, Firewall Location and Configurations. Blockchains, Cloud Security and IoT security

Textbooks
1. Cryptography and Network Security: Principles and Practice, 6th Edition, William Stallings, 2014, Pearson, ISBN 13:9780133354690.

References
1. Network Security: Private Communications in a Public World, M. Speciner, R. Perlman, C. Kaufman, Prentice Hall, 2002.
2. Linux iptables Pocket References, Gregor N. Purdy, O'Reilly, 2004, ISBN-13: 978- 0596005696.
3. Linux Firewalls, by Michael Rash, No Starch Press, October 2007, ISBN: 978-1-59327-141-1.
4. Network Security, Firewalls and VPNs, J. Michael Stewart, Jones & Bartlett Learning, 2013, ISBN-10: 1284031675, ISBN-13: 978-1284031676.

Course Code: **CSE503C**	**Machine Learning**	Credits: **03** L T P 3 0 0

Course Outcomes
- Develop a comprehensive understanding of core machine learning concepts, including the difference between supervised, unsupervised, and reinforcement learning approaches.
- Gain hands-on experience and understanding of essential algorithms such as linear regression, logistic regression, support vector machines, decision trees, and neural networks.
- Acquire the skills to process and prepare data for machine learning, including techniques for dealing with missing data, variable transformation, feature selection, and dimensionality reduction.
- Learn to rigorously evaluate machine learning models using appropriate metrics and validation techniques such as confusion matrices, cross-validation, and ROC curves.

Unit I
Definitions of Probability: Classical, Relative Frequency, and Axiomatic Approaches, Probability Rules: Addition, Multiplication, and Conditional Probability, Bayes' Theorem, Independent Events, Probability Distributions: Discrete and Continuous, Mathematical Techniques: Linear Algebra and Optimization.

Unit II
Vector Spaces: Fundamentals, subspaces, and spanning sets, Linear Combinations: Construction and representation of vectors, Linear Dependence and Independence, Basis and Dimension, Inner-Product Spaces, Linear Transformations and Matrices: Matrix representations, transformations, and their properties, Eigenvalues and Eigenvectors, Rank, Nullity, and Inverses, Optimization Techniques: Key methods for machine learning, including gradient-based approaches.

Unit III
Linear Models: Linear Regression, Logistic Regression, Multi-class Regression, SoftMax Regression, Bayesian Methods: Bayes Classifier, Naïve Bayes, Support Vector Machines, Key Concepts and Techniques: Bias-Variance Trade-off, Model Validation (training, validation, test split, cross-validation) Regularization: Techniques to prevent overfitting and improve generalization.

Unit IV
Decision Trees and Attribute Selection, Neural Networks and Backpropagation, Ensemble Learning Methods (boosting, bagging, and random forest), Curse of Dimensionality techniques, Feature Selection Techniques, Introduction to Unsupervised Learning: Clustering and k-Means Algorithms.

Unit V
Evaluation metrics (ROC curve, precision-recall); Semi-supervised and Reinforcement Learning; Graphical Models, Machine Learning for IoT applications, Current trends in machine learning, Transfer Learning, Ethical considerations in AI.

Textbooks
1. Introduction to Machine Learning, Edition 2, by Ethem Alpaydin
2. Pattern recognition and machine learning by Christopher Bishop
3. Hands-On Machine Learning with Scikit-Learn and TensorFlow, O'Reilly, Aurélien Géron

References
1. The Hundred-Page Machine Learning Book by Andriy Burkov.
2. Machine Learning with Python Cookbook

Online Resources
1. https://www.coursera.org/specializations/machine-learning
2. https://course.fast.ai

Course Code: **CSE504C**	**Cyber Physical Systems**	Credits: **03** L T P 3 0 0

Course Outcomes
- To introduce the foundational principles and architecture of Cyber Physical Systems (CPS).
- To identify CPS components, design challenges, and integration strategies.
- To explore CPS enabling technologies such as sensors, actuators, and embedded platforms.
- To understand cloud connectivity, data analytics, and security in CPS.
- To apply CPS models to real-world applications across domains like smart cities and healthcare.

Unit I: Introduction to Cyber Physical Systems
Definition, characteristics, architecture of Cyber Physical Systems (CPS). CPS in Industry 4.0 and IIoT. Challenges and design considerations in CPS. Physical and logical design, CPS functional blocks. Applications in healthcare, energy, and transportation.

Unit II: Hardware Platforms and Enabling Technologies
Microcontrollers, microprocessors, ADC/DAC. Sensors: motion, pressure, temperature, humidity. Enabling tech: RFID, SCADA, WSN. Endpoints, control units, communication modules. CPS architectural pillars: sensing, computation, control, communication.

Unit III: Deployment and Communication in CPS
Arduino, Raspberry Pi-based prototyping. Sensor interfacing and real-world data collection. Mobile-device integration: USB, Wi-Fi, Bluetooth. Network configuration and scalability. Routing protocols: CTP, LOADng.

Unit IV: Data Management and Security
Cloud-based data processing and analytics. REST APIs and Richardson Maturity Model. Lightweight encryption techniques (ECC, AES). Cloud access control and authentication. Quadruple trust model for CPS security.

Unit V: CPS Applications and Business Use Cases
CPS in smart cities, fleet management, retail. Smart farming, green buildings, and infrastructure. Healthcare monitoring systems. Business models for deploying CPS solutions. Case studies in scalable CPS deployments.

Textbooks
1. Edward A. Lee & Sanjit A. Seshia, Introduction to Embedded Systems: A Cyber-Physical Systems Approach, 2nd Edition, http://LeeSeshia.org

References
1. Rajeev Alur, *Principles of Cyber-Physical Systems*, MIT Press
2. Simone Cirani et al., *Internet of Things: Architectures, Protocols and Standards*, Wiley
3. Jane W.S. Liu, *Real-Time Systems*, Prentice Hall.
4. Mark H. Klein et al., *Practitioner's Handbook for Real-Time Analysis*, Kluwer Academic

Online Resource
1. NPTEL – Cyber Physical Systems: https://nptel.ac.in/courses/106/105/106105195

Course Code: **CSE505C**	**Research Methodology**	Credits: **03** L T P 3 0 0

Course Outcomes
- Understand the definition and objectives of research, and the various types of research methodologies.
- Learn how to define and formulate a research problem, and the importance of literature review in this process.
- Explore different research designs, methods, and the development of research plans.
- Gain knowledge of data collection methods, sampling techniques, and data analysis strategies using statistical packages.
- Learn the structure and components of scientific reports, and the different steps involved in preparing reports and thesis writing.

Unit I
Introduction: Definition and objectives of Research, Various Steps in Research process. Types of research: Descriptive vs. Analytical, Applied vs. Fundamental, Quantitative vs. Qualitative, and Conceptual vs. Empirical.

Unit II
Research Formulation: Defining and formulating the research problem, Selecting the problem, Necessity of defining the problem, Importance of literature review in defining a problem. Literature review: Primary and secondary sources, reviews, treatise, monographs, patents, web as a source, searching the web. Critical literature review: Identifying gap areas from literature review

Unit III
Research design and methods: Research design, Need of research design, Features of good design, Observation and Facts, Laws and Theories, Prediction and explanation, Induction, Deduction, Development of Models. Developing a research plan Exploration, Description, Diagnosis and Experimentation.

Unit IV
Data Collection and analysis: Execution of the research, Observation and Collection of data. Methods of data collection: Sampling Methods, Data Processing and Analysis strategies, Data Analysis with Statistical Packages

Unit V
Reporting and thesis writing: Structure and components of scientific reports, Types of report, Technical reports and thesis, Significance. Different steps in the preparation: Layout, structure and Language of typical reports, Illustrations and tables, Bibliography, referencing and footnotes.

Textbooks
1. Kothari, C.R., 1990. Research Methodology: Methods and Techniques.
2. B. L. Garg, R. Karadia, F. Agarwal. An introduction to Research Methodology, RBSA Publishers. References
3. Donald H. McBurney, Research Methods, 5th Edition, Thomson Learning

Course Code: **CSE506C**	**Advanced Network Security Lab**	Credits: **01** L T P 0 0 2

Course Outcomes
- Apply cryptographic algorithms, hashing, and digital signatures to secure data and communications.
- Evaluate key management schemes and authentication protocols for secure identity verification.
- Implement network and transport layer security mechanisms such as IPsec, TLS/SSL, and SSH.
- Analyze and apply security techniques for email, wireless, and mobile communication systems.
- Configure firewalls, intrusion detection systems, and explore Blockchain, Cloud, and IoT security.

List of Practicals

1. Implement classical ciphers (Caesar/Vigenère) and perform cryptanalysis using frequency analysis.

2. Demonstrate how to ensure file integrity using cryptographic hash functions (MD5, SHA-256).

3. Implement message authentication and digital signature generation using GnuPG/OpenSSL tools.

4. Demonstrate how to perform symmetric key distribution and compare it with Diffie–Hellman key exchange.

5. Study of the features of a firewall in providing network security and to set Firewall Security in Windows.

6. Secure email communication using PGP and S/MIME protocols.

7. Configure and manage host-based and network-level firewalls using open-source firewall tools.

8. Detect and analyse network intrusions by configuring intrusion detection systems.

9. Understand blockchain-based mechanisms to ensure file integrity and verification.

10. Understand secure communication in IoT systems using encryption and access control mechanisms.

Course Code: **CSE507C**	**Machine Learning Lab**	Credits: **01** L T P 0 0 2

Course Outcomes
- Develop a comprehensive understanding of core machine learning concepts, including the difference between supervised, unsupervised, and reinforcement learning approaches.
- Gain hands-on experience and understanding of essential algorithms such as linear regression, logistic regression, support vector machines, decision trees, and neural networks.
- Acquire the skills to process and prepare data for machine learning, including techniques for dealing with missing data, variable transformation, feature selection, and dimensionality reduction.

List of Practicals

1. Implement linear regression on a dataset to predict housing prices based on features like square footage, number of bedrooms, etc.

2. Use logistic regression to predict whether a customer will churn or not based on their historical data.

3. Apply multi-class regression to classify handwritten digits from the MNIST dataset.

4. Implement SoftMax regression to classify iris flower species based on sepal and petal measurements.

5. Use a Bayes classifier to classify emails as spam or not spam based on their content.

6. Implement Naïve Bayes for sentiment analysis on movie reviews dataset.

7. Implement linear SVM classification on a binary classification dataset such as the Iris dataset to distinguish between two classes of flowers.

8. Implement k-fold cross-validation to assess the performance of a SVM model on a dataset.

9. Compare the performance of a linear regression model with and without L1/L2 regularization on a dataset with multicollinear features.

10. Use information gain and Gini index to select attributes for decision tree classification on a dataset like the Titanic survival dataset.

Course Code: **CSE508C**	**Cyber Physical Systems Lab**	Credits: **01** L T P 0 0 2

Course Outcomes
- Design and implement a basic Cyber Physical System (CPS) model using Arduino and sensors for real-time data acquisition and processing.
- Develop skills in interfacing and controlling actuators based on sensor thresholds in a CPS environment.
- Configure wireless communication (Bluetooth/Wi-Fi) to transmit CPS data securely to mobile or cloud platforms.
- Create and deploy real-time CPS dashboards for data visualization using cloud-based IoT platforms.
- Build a secure smart home CPS mini-project integrating sensors, actuators, and encrypted communication.

List of Practicals

1. Setting up a basic CPS model using Arduino and temperature sensor.

2. Real-time data acquisition from motion or light sensors.

3. Displaying sensor data on serial monitor and LCD.

4. Controlling an actuator (motor/LED) using sensor threshold.

5. Bluetooth-based data transmission from CPS to mobile device.

6. Uploading sensor data to cloud (ThingSpeak/AWS IoT).

7. Implementing REST API calls to trigger actions.

8. Basic encryption of sensor data before transmission.

9. Creating a CPS dashboard for real-time data visualization.

10. Mini-project: Smart home lighting and monitoring CPS with security features.

SEMESTER II – CORE COURSES

Course Code: **CSE550C**	**Advanced Computer Architecture**	Credits: **03** L T P 3 0 0
Course Outcomes • Provide knowledge on instruction level parallelism • Describe the hardware and software level parallelism to enhance the computing performance • Describe the different operations of performance enhancement such as pipelines, dynamic scheduling, branch prediction, caches, and vector processors • Design the models for arithmetical calculation and to evaluate the CPU performance • Understand the memory hierarchy model for enhanced computing performance		

Unit I
Overview of Parallel Processing and Pipelining Processing, comparison of uni-processors and parallel processors. Evolution of parallel processors, future trends and their architecture, Architectural Classification, Applications of parallel processing, Instruction level Parallelism and Thread Level Parallelism, Explicitly Parallel Instruction Computing (EPIC) Architecture.

Unit II
Principles and implementation of Pipelining, Classification of pipelining processors, Pipeline Architecture, Study and comparison of processors with and without pipelining. General pipelining reservation table, Pipelining hazards and resolving techniques, Data buffering techniques, Job sequencing and Collision.

Unit III
Study and comparison of Vector and array processors, Vector and Array Processor, Basic vector architecture, Issues in Vector Processing, Vector performance modeling, vectorizers and optimizers.

Unit IV
Microprocessor Architectures, study and comparison of Loosely and Tightly coupled multiprocessors. Processor characteristics of multiprocessors, Inter Processor communication network, Time shared bus, Crossbar switch, Multiport Memory Model, Memory contention and arbitration techniques.

Unit V
Study of Architecture of Multithreaded processors, Latency hiding techniques, Principles of multithreading, Issues, and solutions. Parallel Programming Techniques: Message passing program development, Synchronous and asynchronous message passing, Message passing parallel programming, Shared Memory Programming.

Textbooks
1. Kai Hwang, Faye A. Briggs, "Computer Architecture and Parallel Processing" McGraw-Hill international Edition
2. Kai Hwang, "Advanced Computer Architecture", Tata McGraw-Hill

References
1. V.Rajaraman, L Sivaram Murthy, "Parallel Computers", PHI.
2. William Stallings, "Computer Organization and Architecture, Designing for performance" Prentice Hall,Sixth edition.
3. Kai Hwang, Scalable Parallel Computing.
4. Harrold Stone, High performance computer Architecture.
5. Richard Y. Kain, Advanced Computer Architecture

Course Code: **CSE551C**	**Advanced Data Structures and Algorithms**	Credits: **03** L T P 3 0 0

Course Outcomes
- Identify and describe various types of algorithms, classify the problems and solve or optimize the problem using the algorithmic approach.
- Analyze the efficiency and correctness of algorithms. Compare and contrast algorithms, identifying trade-offs and concerns including more than just running time.
- Classify an algorithm as a greedy algorithm, brute force, dynamic program, divide and conquer algorithm, etc.
- Develop working programs demonstrating application of algorithms.
- Demonstrate how different algorithmic approaches affect the performance. Apply algorithm design techniques to create an algorithm that solve a problem.

Unit I
Introduction to Algorithms, Mathematical Structures, Logarithms, Series, Induction, Analysing Algorithms, Asymptotic Analysis.

Unit II
Recurrences, Recursion Trees, Master Method, Divide and Conquer Algorithms

Unit III
Binary Trees, Order Traversals, BST Property, Heaps & Priority Queues, Heap Sort, Graph Algorithms, BFS, DFS, DAG, Topological Sort, Minimal Spanning Trees, Shortest Path

Unit IV
Dynamic Programming, Memorization, Elements of DP, LCS, Greedy Algorithms, Activity Selection, Fractional Knapsack

Unit V
NP Completeness, Polynomial time verification, Reducibility, SAT, HAM-Cycle

Textbooks
1. Introduction to Algorithms (Third Edition) By Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein

Course Code: **CSE552C**	**Data Analytics using Python**	Credits: **01** L T P 0 0 2

Course Outcomes

- Apply Python-based tools to perform data acquisition, exploratory data analysis (EDA), and preprocessing techniques for structured datasets.
- Analyze datasets using appropriate statistical methods including hypothesis testing, correlation analysis, and ANOVA to derive meaningful inferences.
- Design and implement regression and classification models, and evaluate their performance using appropriate statistical and machine learning metrics.
- Apply unsupervised learning techniques such as clustering and dimensionality reduction to extract patterns and structure from high-dimensional data.
- Develop and validate end-to-end data analytics pipelines, including time series forecasting and model interpretation, for solving real-world analytical problems.

1. **Data Loading and Exploration:** Load datasets using pandas (CSV/Excel/JSON formats). Perform exploratory data analysis (EDA) including summary statistics, data types inspection, missing value detection, and basic visualization.

2. **Data Preprocessing and Cleaning:** Handle missing values, remove duplicates, perform feature scaling (Normalization/Standardization), encoding of categorical variables, and outlier detection.

3. **Data Visualization Techniques:** Create various plots using Matplotlib and Seaborn such as histograms, boxplots, scatter plots, heatmaps, pair plots, and correlation matrices.

4. **Statistical Analysis using Python:** Perform descriptive and inferential statistics including mean, variance, hypothesis testing (t-test, chi-square test), correlation analysis, and ANOVA.

5. **Regression Analysis:** Implement Linear Regression and Multiple Linear Regression using scikit-learn. Evaluate model performance using R^2 score, MSE, RMSE, and MAE.

6. **Classification Techniques:** Apply classification algorithms such as Logistic Regression, k-Nearest Neighbors (kNN), Decision Trees, and Support Vector Machines. Evaluate using confusion matrix, precision, recall, F1-score, and ROC curve.

7. **Clustering Algorithms:** Implement clustering techniques such as K-Means and Hierarchical Clustering. Use silhouette score and dendrogram analysis for evaluation.

8. **Dimensionality Reduction:** Apply Principal Component Analysis (PCA) for dimensionality reduction and visualize high-dimensional datasets in 2D/3D space.

9. **Time Series Analysis:** Perform time series decomposition, moving averages, and forecasting using ARIMA or other suitable models on real-world datasets.

10. **Mini Project: End-to-End Data Analytics Pipeline:** Develop a complete analytics pipeline including data collection (if possible), preprocessing, visualization, model building, evaluation, and interpretation on a real-world dataset (e.g., healthcare, finance, or social media data).

Course Code: **CSE553C**	**Advanced Data Structures and Algorithms Lab**	Credits: **01** L T P 0 0 2

Course Outcomes
- Analyze the time and space complexity of algorithms using asymptotic notations and recurrence relations.
- Design and implement efficient algorithms using divide-and-conquer and graph-based techniques.
- Apply advanced data structures such as trees, heaps, and graphs to solve computational problems.
- Develop dynamic programming and greedy solutions for optimization problems and compare their effectiveness.
- Explain the theory of NP-completeness, polynomial-time verification, and problem reducibility in computational complexity.

List of Practicals

1. Implement and empirically analyze linear search, binary search, and merge sort to compare their time complexities for varying input sizes.

2. Implement merge sort and derive its recurrence relation, then verify the solution using the Master Theorem and runtime measurements.

3. Implement a Binary Search Tree (BST) and evaluate its height and search performance for random and sorted input sequences.

4. Implement a binary heap and use it to perform heap sort and priority queue operations on a dataset.

5. Implement Breadth First Search (BFS) and Depth First Search (DFS) to traverse a graph and analyze their performance on sparse and dense graphs.

6. Implement topological sorting using both DFS-based approach and Kahn's algorithm on a directed acyclic graph (DAG).

7. Implement Kruskal's and Prim's algorithms to find the Minimum Spanning Tree (MST) of a weighted graph and compare their efficiencies.

8. Implement the Longest Common Subsequence (LCS) problem using dynamic programming and analyze its time and space requirements.

9. Implement Fractional Knapsack using a greedy approach and compare it with the 0/1 Knapsack problem solved using dynamic programming.

10. Implement a polynomial-time verification algorithm for a given solution to the SAT or Hamiltonian Cycle problem and analyze its computational complexity.

ELECTIVE COURSES

VERTICAL 1:
CYBER SECURITY

CSE566E	**Applied Cryptography**	Credits: 03 L T P 3 0 0

| **Course Outcomes** |
| • Interpret the basic principles of cryptography and general cryptanalysis.
• Determine the concepts of symmetric encryption and authentication.
• Identify the use of public key encryption, digital signatures, and key establishment.
• Articulate the cryptographic algorithms to compose, build and analyze simple cryptographic solutions.
• Express the use of Message Authentication Codes. |

Unit I
Basics of Symmetric Key Cryptography, Basics of Asymmetric Key Cryptography, Hardness of Functions. Notions of Semantic Security (SS) and Message Indistinguishability (MI): Proof of Equivalence of SS and MI, Hard Core Predicate, Trap-door permutation, Goldwasser-Micali Encryption. Goldreich-Levin Theorem: Relation between Hardcore Predicates and Trap-door permutations.

Unit II
Cryptographic Protocols – Key exchange protocols, Multiple-Key Public Key Cryptography (RABIN, ELGAMAL, ECC), Timestamping Services, Undeniable digital signatures, Fair Coin Flips, Zero Knowledge Proofs, Identity based Public Key Cryptography, Digital Certified Mail.

Unit III
Information theory, Complexity theory, Number Theory, Discrete Logarithms in a Finite Field, Pseudo-random Generators (PRG): Blum-Micali-Yao Construction,Construction of more powerful PRG, Relation between One-way functions and PRG, Pseudorandom Functions (PRF)

Unit IV
Cryptographic Techniques – Key Management Techniques, Authentication techniques, Electronic Codebook Mode, Cipher Block Chaining mode, Cipher Feedback Mode, Output Feedback mode, Counter mode, Self-Synchronizing Stream Ciphers, choosing a Cipher mode, Hardware Encryption vs Software Encryption, Encrypting Data for storage, Destroying Information.

Unit V
Left or Right Security (LOR). Formal Definition of Weak and Strong MACs, Using a PRF as a MAC, Variable length MAC. Public Key Signature Schemes: Formal Definitions, Signing and Verification,

Textbooks
1. Applied Cryptography, Protocols, Algorithms and Source Code in C, by Bruce Schneier, Wiley.
2. Cryptography, Theory and Practice, by Douglas R. Stinson, Chapman & Hall, CRC, Taylor and Francis Group.

References
1. ShaffiGoldwasser and MihirBellare, Lecture Notes on Cryptography, Available at http://citeseerx.ist.psu.edu/.
2. OdedGoldreich, Foundations of Cryptography, CRC Press (Low Priced Edition Available),
3. William Stallings, "Cryptography and Network Security: Principles and Practice", PHI 3rd Edition, 2006.

CSE551E	**Wireless and Mobile Security**	Credits: 04 L T P 3 0 2

Course Outcomes
- Gain knowledge on Security and Privacy topics in wireless and mobile networking
- Understand the security and Privacy problems in the realm of wireless networks and mobile computing
- Gain knowledge and understanding of the various ways in which wireless networks can be attacked and tradeoffs in protecting networks
- Analyze the various categories of threats, vulnerabilities, and countermeasures in the area of wireless and mobile networking
- Designing secured wireless and mobile networks that optimize accessibility whilst minimizing vulnerability to security risks

Unit I
Introduction to wireless networks security: Wired vs. wireless network security, Threat categories and the OSI model, Vulnerabilities, Countermeasures, Security architectures. IEEE 802.11 standard security issues: Authentication and authorization mechanisms, Confidentiality and Integrity, pre-RSNA protocols (WEP), RSNA (802.11), Key management, Threat analysis and case studies. Mobile networks security.

Unit II
Overview of Wireless security, Scanning and Enumerating 802.11 Networks, Attacking, 802.11 Networks, Attacking WPA protected 802.11 Networks, Bluetooth Scanning and Reconnaissance, Bluetooth Eavesdropping, Attacking and Exploiting, Bluetooth, Zigbee Security, Zigbee Attacks.

Unit III
Security in Ad Hoc Wireless Networks, Network Security Requirements, Issues, and Challenges in Security Provisioning, Network Security Attacks, Key Management in Adhoc Wireless Networks, Secure Routing in Adhoc Wireless Networks.

Unit IV
Mobile system architectures, Overview of mobile cellular systems, GSM and UMTS, Security architecture & Attacks, Vulnerabilities in Cellular Services, Cellular Jamming, Attacks & Mitigation, Security in Cellular VoIP Services, Mobile application security.

Unit V
Android vs. IoS security model, threat models, information tracking, rootkits, Threats in mobile applications, analyzer for mobile apps to discover security vulnerabilities, Viruses, spywares, and keyloggers and malware detection.

Textbooks
1. S. Kami Makki, Peter Reiher, Kia Makki, Niki Pissinou, Shamila Makki, "Mobile and Wireless Network Security and Privacy", Springer, ISBN 978-0-387-71057-0, 09-Aug-2007
2. Anurag Kumar, D. Manjunath, Joy Kuri "Wireless Networking" Morgan Kaufmann Publishers, First edition, 2009.

References
1. C. Siva Ram Murthy, B.S. Manoj, "Adhoc Wireless Networks Architectures and Protocols", Prentice Hall, ISBN 9788131706885, 2007
2. Noureddine Boudriga, "Security of Mobile Communications", ISBN 9780849379413, 2010.
3. Kitsos, Paris; Zhang, Yan, "RFID Security Techniques, Protocols and System- On-Chip Design ", ISBN 978-0-387-76481-8, 2008.
4. Johny Cache, Joshua Wright and Vincent Liu," Hacking Wireless Exposed:Wireless Security Secrets & Solutions", second edition, McGraw Hill, ISBN: 978-0-07-166662-6, 2010.

CSE567E	**Secure Systems Architecture and Design**	Credits: 03 L T P 3 0 0

Course Outcomes
- Understand the principles and concepts of secure systems architecture and design.
- Identify and analyze security threats and vulnerabilities in systems.
- Design and implement secure systems using appropriate security measures and best practices.
- Apply cryptographic techniques for data protection and secure communication.
- Evaluate and assess the security of existing systems and propose improvements

Unit I
Overview of secure systems architecture, Importance of security in system design, Threat modeling and risk assessment, Security standards and best practices, Case studies of security breaches.
Cryptography Fundamentals.

Unit II
Network security principles, Secure communication protocols (SSL/TLS, IPsec), Firewalls and intrusion detection/prevention systems, Virtual Private Networks (VPNs), Denial of Service (DoS) mitigation techniques.

Unit III
Secure coding principles, Common vulnerabilities (SQL injection, XSS, CSRF), Static and dynamic code analysis, Secure development frameworks and libraries, Secure software development lifecycle (SDLC).

Unit IV
Access control models (DAC, MAC, RBAC), Authentication methods (passwords, biometrics, tokens), Single Sign-On (SSO) and federated identity management
Role-based access control, Identity and access management (IAM) systems.

Unit V
Introduction to IoT systems, IoT architecture and components, Security challenges in IoT, IoT authentication and access control, IoT security protocols and standards.
Emerging trends in secure systems.

Textbooks
1. "Security Engineering: A Guide to Building Dependable Distributed Systems" by Ross Anderson
2. "Building Secure Software: How to Avoid Security Problems the Right Way" by John Viega and Gary McGraw.

References
1. "Computer Security: Principles and Practice" by William Stallings and Lawrie Brown
2. "Cryptography and Network Security: Principles and Practice" by William Stallings
3. "Security in Computing" by Charles P. Pfleeger, Shari Lawrence Pfleeger, and Jonathan Margulies

CSE553E	**Cybersecurity Attack and Defense Fundamentals**	Credits: 04 L T P 3 0 2

Course Outcomes
- Understand the basics of cyber security, cybercrime and cyber law.
- Classify various types of attacks and learn the tools to launch the attacks.
- To analyze common methods used to secure cyber-physical systems.
- Apply intrusion techniques to detect intrusion.
- Apply intrusion prevention techniques to prevent intrusion.

Unit I

Cyber Security – Impact of Internet – CIA Triad; Reason for Cyber Crime –Need for Cyber Security – History of Cyber Crime; Cybercriminals – Classification of Cybercrimes – A Global Perspective on Cyber Crimes; Cyber Laws – The Indian IT Act – Cybercrime and Punishment.
Web attack: Browser Attacks, Web Attacks Targeting Users, Obtaining User or Website Data, Email Attacks. Network Vulnerabilities.

Unit II

OSWAP; Malicious Attack Threats and Vulnerabilities: Scope of Cyber-Attacks – Security Breach – Types of Malicious Attacks – Malicious Software – Common Attack Vectors – Social engineering Attack – Wireless Network Attack – Web Application Attack – Attack Tools – Countermeasures

Unit III

Host -Based Intrusion Detection – Network -Based Intrusion Detection – Distributed or Hybrid
Intrusion Detection – Intrusion Detection Exchange Format – Honeypots – Example System Snort.

Unit IV

Firewalls and Intrusion Prevention Systems: Need for Firewalls – Firewall Characteristics and
Access Policy – Types of Firewalls – Firewall Basing – Firewall Location and Configurations – Intrusion Prevention Systems – Example Unified Threat Management Products.

Unit V

Open Access to Organizational Data, Weak Authentication, Unprotected Broadband communications, Poor Cyber Security Awareness. Cyber Security Safeguards. Policy issues in security management Managing and securing critical infrastructure, policies, access control and formal methods

Textbooks
1. John R.Vacca, Computer and Information Security Handbook, Second Edition, Elsevier 2013.
2. Richard E.Smith, Elementary Information Security, Second Edition, Jones and Bartlett Learning, 2016
3. Anand Shinde, "Introduction to Cyber Security Guide to the World of Cyber Security", Notion Press, 2021

References
1. David Kim, Michael G. Solomon, "Fundamentals of Information Systems Security", Jones & Bartlett Learning Publishers, 2013.
2. Patrick Engebretson, "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made easy", Elsevier, 2011.
3. Kimberly Graves, "CEH Official Certified Ethical hacker Review Guide", Wiley Publishers, 2007

CSE550E	**Python for Cybersecurity**	Credits: 04 L T P 3 0 2

Course Outcomes
- Demonstrate proficiency in Python programming for cybersecurity tasks.
- Utilize Python scripts for pinging targets, including multiple targets.
- Implement basic cryptographic techniques, such as Caesar Cipher and ROT13, in Python.
- Utilize cybersecurity APIs and web scraping techniques for cybersecurity tasks.

Unit 1

Interactive Python, Variables in Python, Hello World, Debugging Python scripts, Additional Debugging of Python code

Unit II

Importing modules/libraries, Using the "os" module to ping, First ping script, Using conditionals, A portable ping script, Using Loops, Pinging multiple targets, Creating and using Functions, Writing to files, Reading from files, Alternative method of pinging

Unit III

Caesar Cipher and the ASCII table, ROT13, Creating ROT13 Python script, Pseudo Encryption Base64 encoding, Using Python Encryption Libraries, How passwords are stored, Hashing passwords in Linux, Performing a Dictionary Attack, Performing a Brute-Force Attack, Encryption using Python Libraries

Unit IV

Ensuring you have a secure password Postman, Ensuring you have a secure password Python, Scanning for viruses API, Scanning for viruses Postman, Scanning for viruses Python, Finding Cybersecurity related APIs, Introduction to APIs, People in space API, JSON, Accessing the GitHub API, Storing API passwords/keys/tokens, Dad jokes API, Using APIs for Cybersecurity tasks

Unit V

Introduction to Web Scraping, Using Python Libraries for Web Scraping, Scraping Security Information from Websites, Scraping Vulnerability Data, Scraping for Threat Intelligence, Ethics and Legal Considerations in Web Scraping for Cybersecurity

Textbooks
1. Python for Automating Information Security. by Thomas McNeela.
2. Python for Security and Networking Third Edition. by José Manuel Ortega.
3. Python Ethical Hacking from Scratch. by Fahad Ali Sarwar.
4. Mastering Python for Networking and Security Second Edition. by José Ortega.

CSE552E	**Network Forensics and Intrusion Detection**	Credits: 04 L T P 3 0 2

Course Outcomes
- To understand basic network forensics and intrusion detection techniques.
- To understand digital crime and investigation.
- To understand how to be prepared for network forensic readiness.
- Describe the characteristics and Demonstrate how to conduct traffic flow analysis.
- Understanding Intrusion detection.

Unit I
Forensic Science – Digital Forensics – Digital Evidence – The Digital Forensics Process – Introduction – The Identification Phase – The Collection Phase – The Examination Phase The Analysis Phase – The Presentation Phase, Network Security Review, Digital Evidence Concepts.

Unit II
Practical Investigation Strategies, Real world cases, Technical fundamentals of digital evidence
Sources of network-based evidence, Principles of internetworking, Internet protocol suite, Physical interception, Traffic acquisition software,

Unit III
Traffic Flow Analysis Protocol analysis, Packet Analysis, Flow Analysis.
Statistical Flow Analysis Collection and aggregation, Flow record export protocols, Analysis
Wireless Forensics Wireless traffic capture and analysis, Common wireless attacks, Locating wireless devices

Unit IV
Network Intrusion Detection and Analysis NIDS/NIPS functionality, Modes of detection, Comprehensive packet logging, Firewalls and Packet Filters: Firewall Basics, Packet Filter Vs
Firewall, how a Firewall Protects a Network, Packet Characteristic to Filter, Stateless Vs Stateful Firewalls, Network Address Translation (NAT) and Port Forwarding.

Unit V
VPN: the basic of Virtual Private Networks, Linux Firewall, Windows Firewall, Snort Intrusion Detection System, Scanning for web vulnerabilities tools: Nikto, W3af.

Textbooks
1. Network Forensics Tracking Hackers Through Cyberspace. Sherri Davidoff & Jonathan Ham. ISBN-13: 978-0132564717

References
2. Linux Firewalls, by Michael Rash, No Starch Press, October 2007, ISBN: 978-1-59327-141-1
3. Network Security, Firewalls And VPNs, J. Michael Stewart, Jones & Bartlett Learning, 2013, ISBN-10: 1284031675, ISBN-13: 978-1284031676.
4. David Kim, Michael G. Solomon, "Fundamentals of Information Systems Security", Jones & Bartlett Learning Publishers, 2013.
5. Patrick Engebretson, "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made easy", Elsevier, 2011.

CSE568E	**Quantum Cryptography and Information Security**	Credits: 03 L T P 3 0 0

Course Outcomes
- Understand the principles of quantum mechanics relevant to cryptography.
- Analyze different quantum key distribution protocols and their security properties.
- Explore the applications of quantum cryptography in secure communication.
- Investigate the challenges and solutions in quantum-resistant cryptography.
- Evaluate the potential impact of quantum computing on information security

Unit I
Introduction to quantum mechanics, Quantum states and operators, Quantum entanglement and superposition, Basics of classical cryptography, Quantum cryptography fundamentals, Principles of quantum key distribution (QKD), BB84 protocol and its variants, Security proofs in quantum cryptography.

Unit II
Quantum entanglement and its properties, Quantum teleportation, Quantum channel capacity and its implications, Quantum error correction.
Quantum-resistant cryptographic algorithms, Post-quantum cryptography: challenges and solutions

Unit III
Practical aspects of QKD systems, Quantum hardware technologies (e.g., quantum key generation devices), Challenges and limitations in implementing quantum cryptography.

Unit IV
Quantum algorithms for cryptanalysis, Shor's algorithm and its impact on classical cryptography, Grover's algorithm and its implications for symmetric key cryptography, Quantum-resistant cryptography: research and development.
Hands-on experience with QKD systems, Simulation of quantum protocols using quantum computing platforms

Unit V
Quantum secure communication networks, Quantum cryptography in IoT and cloud computing
Post-quantum cryptography, Emerging trends and future prospects in quantum cryptography.

Textbooks
1. "Quantum Computation and Quantum Information" by Michael A. Nielsen and Isaac L. Chuang
2. "Quantum Information and Quantum Computing" by Mikio Nakahara and Tetsuo Ohmi
3. "Quantum Cryptography and Secret-Key Distillation" by Louis Salvail and Josep Domingo-Ferrer

References
1. "Quantum Cryptography and Information Security" by T. R. G. Nair
2. "Post-Quantum Cryptography" by Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen3. Kitsos, Paris; Zhang, Yan, "RFID Security Techniques, Protocols and System- On-Chip Design ", ISBN 978-0-387-76481-8, 2008.

CSE569E	**Cyber Threat Intelligence**	Credits: 03 L T P 3 0 0

Course Outcomes
- Understand Cyber Threat Intelligence fundamentals and methodologies comprehensively.
- Proficiently utilize diverse threat intelligence sources and tools.
- Apply structured analytical techniques for effective threat intelligence analysis.
- Integrate threat intelligence into cybersecurity operations and strategic decision-making.
- Identify and address emerging cyber threats, enhancing organizational resilience.

Unit I
Understanding the concept of threat intelligence, Evolution and importance of cyber threat intelligence, Role of threat intelligence in cybersecurity, Types of threat intelligence (strategic, tactical, operational), Cyber threat intelligence lifecycle.

Unit II
Overview of threat actors (hackers, state-sponsored groups, hacktivists, insiders), Motivations and objectives of threat actors, Tactics, techniques, and procedures (TTPs) employed by threat actors, Attribution challenges in cyber threat intelligence

Unit III
Open-source intelligence (OSINT), Closed-source intelligence (CSINT).
Introduction to Threat Intelligence Platforms (TIPs), Common features and functionalities of TIPs, Threat feeds and data sources, Automated threat intelligence collection and analysis tools
Hands-on experience with popular threat intelligence tools.

Unit IV
Integrating threat intelligence into incident response processes, Threat hunting and proactive threat detection, Incident triage and prioritization using threat intelligence, Case studies and real-world examples of threat intelligence-driven incident response.

Unit V
Analysis of current cyber threat landscape, Emerging threats and attack vectors, Advanced persistent threats (APTs) and nation-state actors, Impact of emerging technologies on threat intelligence.

Textbooks
1. "Threat Intelligence: Inside the Mind of the Cybercriminal" by Tyler Moffitt and W. K. Peek
2. "The Threat Intelligence Handbook: A Practical Guide for Security Teams to Unlocking the Power of Intelligence" by Recorded Future

References
1. "Cybersecurity for Executives: A Practical Guide" by Gregory J. Touhill and C. Joseph Touhill
2. "Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information" by Michael Bazzell.

CSE601E	**Penetration Testing, Incident Response and Forensics**	Credits: 04 L T P 3 0 2

Course Outcomes
- To understand the basic principles for Information Gathering and Detecting Vulnerabilities in the system
- Gain knowledge about the various attacks caused using the network and communication system in an application
- Ability to determine the security threats and vulnerabilities in computer networks using penetration testing techniques
- Demonstrate the knowledge of forensic examination related to Microsoft Windows and Linux artifacts
- Analyze different disk drives and file systems used in different operating systems
- Apply various tools during real world forensic investigation

Unit I
Introduction Terminologies Categories of Penetration Testing Phases of Penetration Test Penetration Testing Reports Information Gathering Techniques Active, Passive and Sources of Information Gathering Approaches and Tools Traceroutes, Neotrace, Whatweb, Netcraft, Xcode Exploit Scanner and NSlookup. Host discovery Scanning for open ports and services Types of Port.

Unit II
Vulnerability Scanner Function, pros and cons Vulnerability Assessment with NMAP Testing SCADA environment with NMAP Nessus Vulnerability Scanner Safe Check Silent
dependencies Port Range Vulnerability Data Resources.
SDN Data plane, Control Plane, Application Plane.

Unit III
Overview of Computer Crime, Forensic investigation Process, Types of investigation, Digital Forensic Evidence, Anti-forensics, Computer Forensic Model, Maintaining Professional Conduct, preparing for investigation and conduction, Report Writing, Data recovery, Forensic tools: OSForensics, FTK, WinHex.

Unit IV
Functions, Categorization, Order of Volatility, Admissibility of Evidence, Acquisition and seizure of evidence, Chain of Custody, Storage formats, Image Capturing Process, Image Validation, Imaging tools: ProDiscover, Linux dd command.

Unit V
Clusters and Sectors, FAT File System, FAT Boot Sector, Interpretation using WinHex, FAT Directories, File Allocation Table, File Slack, New Technology File System (NTFS). Encrypting File System (EFS). Examining Linux File Structures, Ext4, Superblocks, Directory entries, Inodes, Data blocks, Leveraging The Sleuth Kit (TSK) and Autopsy, fsslat, mmls, Forensic data from /etc, /usr, /var, /dev, /proc, Timeline Analysis.

Textbooks
1. Rafay Baloch, Ethical Hacking and Penetration Testing Guide, CRC Press, 2015. ISBN: 78-1-4822-3161-8.
2. Dr. Patrick Engebretson, The Basics of Hacking and Penetration Testing Ethical Hacking and Penetration Testing made easy, Syngress publications, Elsevier, 2013. ISBN :978-0-12-411644-3.
3. Bill Nelson Amelia Phillips Christopher Steuart, "Guide to Computer Forensics and Investigations", 4th Edition, Course Technology, Cengage Learning, ISBN-13: 978-1-435-49883
4. Brian Carrier, "File System Forensic Analysis", Pearson education, 1st Edition, ISBN-13:978-0321268174

References
1. Andrew Whitaker and Daniel P. Newman, Penetration Testing and Network Defence The practical guide to simulating, detecting and responding to network attacks, Cisco Press, 2010. ISBN: 1-58705-208-3.
2. Vivek Ramachandran, BackTrack 5 Wireless Penetration Testing, Beginners guide Master bleeding edge wireless testing techniques with BackTrack 5, PACKT Publishing, 2011. ISBN 978-1-849515-58-0.
3. E. Casey, Handbook of Digital Forensics and Investigation, Academic Press, 1st Edition,2010, ISBN-13: 978-0123742674.
4. Dejey, Murugan, Cyber Forensics, Oxford Higher Education, 2018.

CSE620E	**Network Security and Database Vulnerabilities**	Credits: 03 L T P 3 0 0

Course Outcomes
- Gain a comprehensive grasp of network security principles and database vulnerabilities.
- Develop expertise in implementing security measures for networks and databases.
- Acquire analytical capabilities to assess and mitigate risks in network security and database management.
- Securing Database using Encryption and Masking Strategies.
- Understanding Best Practices to Secure Database.

Unit I
Overview of Network Security, Definition, Goals, and Components, Threats and Attacks in Network Security, Cryptography Basics, Symmetric and Asymmetric Encryption, Hash Functions and Digital Signatures, Network Security Protocols. SSL/TLS, IPsec, SSH, VPN Technologies.

Unit II
Firewalls and Intrusion Detection Systems (IDS), Types and Configurations, Packet Filtering and Stateful Inspection, Secure Network Design Principles, DMZ, VLANs, Subletting, Defense-in-Depth Strategies.

Unit III
Introduction to Database Security, Importance and Challenges, Threats to Database Systems, Access Control Mechanisms, Role-Based Access Control (RBAC), Mandatory Access Control (MAC), Database Auditing and Monitoring.

Unit IV
Understanding SQL Injection, Types and Methods of SQL Injection Attacks.
Encryption in Database Systems, Transparent Data Encryption (TDE), Column-Level Encryption, Data Masking Techniques, Dynamic Data Masking (DDM), Static Data Masking.

Unit V
Backup and Recovery Strategies, Database Backup Encryption, Disaster Recovery Planning, Patch Management and Vulnerability Assessment, Database Patching Procedures, Vulnerability Scanning Tools.

Textbooks
1. Cryptography and Network Security: Principles and Practice" by William Stallings
2. Database Security and Auditing: Protecting Data Integrity and Accessibility" by Hassan A. Afyouni

References
1. Firewalls and Internet Security: Repelling the Wily Hacker" by William Cheswick, Steven M. Bellovin, and Aviel D. Rubin.
2. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" by Dafydd Stuttard and Marcus Pinto
3. Oracle Database 12c Security" by Scott Gaetjen and Grant Ronald
4. Securing SQL Server: Protecting Your Database from Attackers" by Peter Carter and Louis Davidson.

CSE619E	**Cyber Security Risk Management Framework**	Credits: 03 L T P 3 0 0

Course Outcomes
- Acquire in-depth knowledge of cybersecurity risk management principles and frameworks.
- Develop skills to identify and prioritize cybersecurity risks effectively.
- Apply practical knowledge to implement effective risk mitigation strategies and security controls.
- Enhance communication abilities to transparently convey cybersecurity risks and mitigation strategies.
- Understanding the trends in the Cyber Security Risk Management.

Unit I
Understanding Cybersecurity Risk, Definition and Components of Cyber Risk, Importance of Risk Management in Cybersecurity, Risk Management Frameworks and Standards.
Overview of NIST Cybersecurity Framework, ISO 27001, and other relevant standards, Comparison of Risk Management Approaches.

Unit II
Risk Identification, Techniques for Identifying Cyber Risks, Asset Valuation and Classification.
Risk Analysis, Qualitative vs. Quantitative Risk Analysis, Risk Likelihood and Impact Assessment.

Unit III
Risk Treatment Options, Risk Acceptance, Avoidance, Mitigation, and Transference, Implementing Controls for Risk Mitigation, Security Controls and Best Practices, Overview of Common Controls (Technical, Administrative, Physical), Secure Configuration Management.

Unit IV
Risk Monitoring Techniques, Continuous Monitoring vs. Periodic Assessments, Key Risk Indicators (KRIs) and Metrics, Risk Reporting and Communication, Effective Communication with Stakeholders, Documentation and Reporting Standards.

Unit V
Cybersecurity Threat Landscape, Current and Emerging Cyber Threats, Impact of Technological Advancements on Risk Management, Future Challenges and Opportunities, Predictive Analytics in Risk Management, Integration of Artificial Intelligence and Machine Learning.
Hands-on Activities to Apply Risk Management Concepts, Use of Simulation Tools for Risk Assessment.

Textbooks
1. Managing Risk and Information Security: Protect to Enable" by Malcolm Harkins
2. Information Security Management Handbook" edited by Harold F. Tipton and Micki Krause

References
1. Communicating Risks and Benefits: An Evidence-Based User's Guide" by Baruch Fischhoff, Noel T. Brewer, and Julie S. Downs.
2. Cybersecurity: A Practical Guide to the Law of Cyber Risk" by David J. Lefort and Paul M. Ferrillo
3. Future Crimes: Inside the Digital Underground and the Battle for Our Connected World" by Marc Goodman
4. Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents" by Eric Cole

CSE604E	**Machine Learning for Cybersecurity**	Credits: 04 L T P 3 0 2
Course Outcomes • Understand the concepts in Machine Learning. • Understand and implement machine learning algorithms and models for CyberSecurity problems such as malware analysis, intrusion detection, spam filtering, fraud detection, online behavior analysis etc. • Learn various AI and Machine learning models for cyber security. • Ability to apply AI and machine learning models in cyber security issues.		

Unit I

Introduction: Role of AI in Cyber Security and Security Framework: Artificial Intelligence in
Cyber Security, Challenges and Promises, Security Threats of Artificial Intelligence, Use-Cases: Artificial Intelligence Email Observing, Programming in Python and Basics of manipulation of Data. Cyber Security Problems and Machine Learning Based Solutions.

Unit II

Basic Probability and Distributions Binomial, Poisson, Normal, Exponential, other distributions, Estimation Theory and Hypothesis Testing, Regression, Supervised Learning Unsupervised Learning, Malware Analysis, Spam Filtering, Adversarial Attacks on spam filters.

Unit III

Machine Learning in Security: Introduction to Machine Learning, Applications of Machine Learning in Cyber Security Domain, Machine Learning: tasks and Approaches, Anomaly Detection, Privacy Preserving Nearest Neighbour Search, Machine Learning Applied to Intrusion Detection, Online Learning Methods for Detecting Malicious Executables

Unit IV

Deep Learning in Security: Introduction to deep learning, Cyber Security Mechanisms Using
Deep Learning Algorithms, Applying deep learning in various use cases, Network Cyber threat
Detection, Training data-poisoning attacks on deep learning, Adversarial input attacks on Deep Learning, Training data and model reconstruction attacks; differential privacy.

Unit V

Artificial Intelligence in Cyber Security: Model Stealing & Watermarking, Network Traffic Analysis, Malware Analysis, Deep fakes and fake news detection, Machine Learning Models for Fraud detection.

References
1. Tom Mitchell. Machine Learning. McGraw Hill, 1997.
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:Neeraj Bhargava, 2021.
4. Tsai, Jeffrey JP, and S. Yu Philip, eds. Machine learning in cyber trust: security, privacy,and reliability. Springer Science & Business Media, 2009.
5. Machine Learning: A Probabilistic Perspective, Kevin P Murphy, MIT Press.

CSE617E	**Cloud Security**	Credits: 03 L T P 3 0 0

Course Outcomes
- Understand the fundamental concepts and principles of cloud computing security.
- Implement security architecture and mechanisms for protecting cloud environments.
- Apply authentication, access control, and encryption techniques to secure cloud resources effectively.
- Evaluate compliance requirements and legal aspects related to cloud security.
- Analyze emerging threats and challenges in cloud security and devise appropriate risk management strategies.

Unit I
Overview of Cloud Computing, Security Challenges in Cloud Computing, Security Benefits of Cloud Computing, Cloud Service Models: IaaS, PaaS, SaaS, Cloud Deployment Models: Public, Private, Hybrid.
Cloud Security Architecture, Virtualization and Container Security, Identity and Access Management (IAM)

Unit II
Network Security in Cloud Environments, Data Security in Cloud Environments,
Authentication Mechanisms in Cloud, Multi-factor Authentication (MFA), Role-based Access Control (RBAC), Access Control Lists (ACLs), Identity Federation

Unit III
Data Encryption Techniques, Key Management in Cloud Environments, Data Loss Prevention (DLP), Secure Data Storage in the Cloud, Cryptography in Cloud Computing.

Unit IV
Risk Assessment in Cloud Computing, Risk Mitigation Strategies, Business Continuity and Disaster Recovery Planning, Incident Response in Cloud Environments, Security Monitoring and Logging. Secure Software Development Lifecycle (SDLC) for Cloud Applications

Unit V
Security Risks of Cloud Adoption, Insider Threats and Data Breaches, Advanced Persistent Threats (APTs), Cloud-specific Attacks (e.g., Side-channel Attacks), Security of IoT Devices in Cloud Environments.

Textbooks
1. "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance" by Tim Mather, Subra Kumaraswamy, Shahed Latif
2. "Cloud Security and Governance: Who's on Your Cloud?" by Tim Mather, Subra Kumaraswamy, Shahed Latif

References
1. "Cloud Computing: Concepts, Technology & Architecture" by Thomas Erl, Ricardo Puttini, Zaigham Mahmood
2. "Architecting Secure Software Systems" by Asoke K. Talukder, Manish Chaitanya
3. "Securing the Cloud: Cloud Computer Security Techniques and Tactics" by Vic (J.R.) Winkler.

CSE618E	**Cybersecurity for Mobile and Web Applications**	Credits: 03 L T P 3 0 0

Course Outcomes
- Understand why mobile application security is essential.
- Learn how to apply appropriate security controls to secure mobile applications, including steps to uplift your security maturity.
- Understanding web application security issues.
- Analyze various security attacks for mobile and web applications.

Unit I

Introduction to Mobile and Web Applications, Security Issues in Mobile Applications, Security Requirements in Mobile Applications, Security techniques for Mobile Applications, Advantages and Disadvantages of Application – level Security.

Unit II

Security obligations and requirements for mobile applications, essential security practices to comply with App Store requirements, Transport Security, Mobile Applications threats and attacks, Data leaks, Memory corruption, Avoiding injection vulnerabilities, Securing Applications with binary protections, Essential security mechanisms.

Unit III

Web Application and Information Gathering HTTP Request, Response, Header Fields and HTTPS, Understanding Same Origin, Cookies, Sessions, Web Application Proxies, Information Gathering: whois, nsLookup, netcraft, web server fingerprinting, subdomain enumeration, fingerprinting frameworks, hidden resource enumeration, security misconfigurations, google hacking database, Shodan HQ.

Unit IV

SQL Injections & Cross Site Scripting SQL Statements, Finding SQL Injections, Exploiting SQL Injections, Bypass Authentication, Xpath Injection, Error Based Injection, Double Query Injection, Time Based injections, Union Based Injections, SQL Map, Mitigation plans, SQLi to Server Rooting, Advance MY-SQL and MS-SQL Exploitation. Cross Site Scripting: Cookie Stealing, Defacements, Advanced Phishing attacks.

Unit V

Multi factor authentication, dictionary and brute force attacks, storing hashes, blocking malicious request, user enumeration, random password guessing, remember me functionality, no limit attempts, password reset feature, logout flaws, CAPTCHA, insecure direct object References and security, Session ID, LFI and RFI ,Session Attacks via packet sniffing or accessing via web server and Fixation, CSRF (Cross Site Request Forgery), Pentesting Flash -based applications, Clickjacking, denial of services attacks.

Textbooks
1. Dominic chell, Tyrone Erasmus, The Mobile Application Hackers' Handbook, Wiley, 1e.

References
1. Mobile Application Security, Himanshu Dviwedi, Chris Clark and David Thiel, 1st Edition
2. Shema, M. & Adam. (2010). Seven deadliest web application attacks. Amsterdam: Syngress Media.
3. Stuttard, D. & Pinto, M. (2011). The web application hacker's handbook: Discovering and exploiting security flaws (2nd ed). Indianapolis, IN: Wiley, John & Sons.
4. Heiderich, M., Nava E.A.V., Heyes, G., & Lindsay, D. (2011). Web application obfuscation. Amsterdam: Syngress Media,U.S.
5. Sullivan, Bryan (2012). Web Application Security, A Beginner's Guide. McGraw- Hill Education.

CSE603E	**Blockchain Security**	Credits: 04 L T P 3 0 2

Course Outcomes
- Understand the basics of blockchain technology and its security implications.
- Explain the role of cryptography in blockchain security, including public-key cryptography and hash functions.
- Analyze consensus algorithms used in blockchain, such as Proof of Work and Proof of Stake, and their security considerations.
- Assess the security of the blockchain ecosystem, including nodes, network security, and attacks on block creation.
- Evaluate smart contracts in terms of security vulnerabilities, best practices, and analysis tools.
- Explore advanced blockchain concepts like distributed ledger architectures, cryptographic protections, and blockchain extensions.

Unit I
Overview of Blockchain Technology, Cryptography in Blockchain, Public-Key Cryptography, Hash Functions, Security Considerations in Blockchain, Physical Ledger Technology and Security, Digital Ledger Technology, Digital Security Technology, Cryptographic Hash Functions, Digital Signatures

Unit II
Introduction to Consensus Algorithms, Principles of Consensus Algorithms, Common Consensus Algorithms (e.g., Proof of Work, Proof of Stake), Security of Consensus Algorithms, Attacks on Consensus Algorithms, BFT problems and solutions, New Consensus mechanisms and their security

Unit III
Blockchain Nodes and Network, Block Creation in Blockchain, Attacks on Block Creation, Attacks on Blockchain Nodes, Network Security in Blockchain, Blockchain Forks and chain resolution, 51% Attack, Anomaly detection and blockchain transactions

Unit IV
Introduction to Smart Contracts, Common Programming Errors in Smart Contracts, Vulnerabilities in Smart Contracts, Ethereum Smart Contract Platform, Best Practices in Smart Contract Development, DAO attacks, Smart Contract Vulnerabilities, Smart contract analysis tools

Unit V
Distributed Ledger Architectures, Advanced Cryptographic Protections, Blockchain Extensions (e.g., Sidechains, Second-Layer Protocols), Improvements to Blockchain Technology, Case Studies and Future Trends in Blockchain Security, Metaverse and Ethical Challenges

Textbooks
1. Cryptographic primitives in blockchain technology: a mathematical introduction by Andreas Bolfing.

References
2. Blockchain-based Internet of Things OpportUnities, Challenges and Solutions Edited By Iraq Ahmad Reshi, Sahil Sholla.
3. Ultimate Blockchain Security Handbook: Advanced Cybersecurity Techniques and Strategies for Risk Management, Threat Modeling, Pen Testing, and Smart Contract Defense for Blockchain by Taha Sajid.

CSE602E	**Cybersecurity for Internet of Things**	Credits: 04 L T P 3 0 2
Course Outcomes • Understand the fundamentals of cyber security, security architecture, threats and vulnerabilities • Familiarize with the different cryptographic algorithms • Understand the network intrusion and its mitigation. • Comprehend the privacy concerns in IoT and SDN. • Understand various cyber-crimes and cyber security.		

Unit I
Cyber security increasing threat landscape, Cyber security terminologies- Cyberspace, attack, attack vector, attack surface, threat, risk, vulnerability, exploit, exploitation, hacker., Non-state actors, Protection of end point devices, Cyber crimes targeting Computer systems and Mobiles- data diddling attacks, spyware, logic bombs, DoS, DDoS, APTs. Cyber Crime and Information Security – classifications of Cyber Crimes.

Unit II
Security and Privacy in Information System, Applied Cryptography & Intrusion Detection, Overview of industrial control systems (ICS), ICS operation & components, Perdue model, SCADA systems, Cyber-physical systems (CPS) & IoT, Architecture of Applied Cryptography, One Way Hash Function and Integrity, Encryption Algorithms and Confidentiality, Digital Signature and Authentication (DH, RSA, 2 class).

Unit III
STRIDE methodology, OWASP IoT vulnerabilities, Privacy & trust, Insufficient authentication/authorization, Insufficient access control, Attacks on IoT data, Attacks on IoT layered architecture, Security concerns in IoT applications, Security concerns in SCADA

Unit IV
Layer wise Security in Internet of Things, Security in IoT Protocols – SMQTT, HTTPS, COAP, XMPP, AMQP, 6LoWPAN, TLs/SSL. Cloud Security – Web Security – Wireless Security

Unit V
Software-Defined Networks, Introduction of Software-Defined Networks, Security for Software-Defined Networks, Privacy Leakages for Software-Defined Networks, Case Studies: How to Attack Software-Defined Networks. Privacy and security in ubiquitous computing, Energy constraints in ubiquitous computing.

References
1. N. Jeyanthi, Ajith Abraham, Hamid Mcheick, "Ubiquitous Computing and Computing Security of IoT".
2. John Krumm, Ubiquitous Computing Fundamentals, CRC Press.
3. Dirk Slama, "Enterprise IoT", Shroff Publisher/O'Reilly Publisher

VERTICAL II:
INTERNET OF THINGS

CSE570E	**Principles of Sensors and Signal Conditioning**	Credits: 03 L T P 3 0 0
Course Outcomes • Understand the Fundamentals of Sensors. • Explore and understand Signal Conditioning Techniques. • Recognize and identify the use of normalization and functional dependency. • Analyze Advanced Signal Conditioning Methods • Apply Sensors and Signal Conditioning in Practical Scenarios.		

Unit I

Overview of Sensors and their Importance, Classification of Sensors: Active and Passive, Analog and Digital, Principles of Operation: Transduction Mechanisms, Sensor Characteristics: Sensitivity, Accuracy, Resolution, Linearity, and Hysteresis, Applications of Sensors in Engineering and Everyday Life

Unit II

Types of errors, Methods of error analysis, Uncertainty analysis, Statistical analysis, Gaussian error distribution, Chi-Square test, Correlation coefficient, Student's t-test, Method of least square, Curve fitting, Graphical analysis

Unit III

Definition, Types, Basic principle and applications of Resistive, Inductive, Capacitive, Piezoelectric and their Dynamic performance. Fiber optic sensors, Bio-chemical sensors, Hall-Effect, Photoemissive, transducers: Principle, Construction, Encoders, Absolute and incremental encoders.

Unit IV

Importance of Signal Conditioning in Sensor Systems, Amplification: Operational Amplifiers and Instrumentation Amplifiers, Filtering Techniques: Low Pass, High Pass, Band Pass, Analog-to-Digital Conversion: ADC Types and Considerations

Unit V

Sensor Networks and Internet of Things (IoT), Automotive Applications: Automotive Sensors and Signal Conditioning, Biomedical Applications: Medical Sensors and Signal Processing, Industrial Automation: Process Control and Monitoring, Environmental Monitoring: Weather Stations, Pollution Sensors

Textbooks

1. Doebelin, E.O. and Manic, D.N., Measurement Systems: Applications and Design, McGraw · Hill.
2. Sawhney, A.K. and Sawhney, P., A Course in Electrical and Electronic Measurements and Instrumentation, Dhanpat Rai (2008).

References

1. Murthy, D.V.S., Transducers and Instrumentation, Prentice Hall of India (2003).
2. Nakra, B.C. and Chaudhry, K.K., Instrumentation, Measurement and Analysis, Tata McGraw Hill.

CSE555E	**Microcontrollers for IoT Prototyping**	Credits: 04 L T P 3 0 2

Course Outcomes
- Design and develop embedded programs for low power microcontrollers for sensor applications.
- Develop ARM basic and advanced programs.
- Interface and deploy analog and digital sensors
- Develop communication system with sensor units
- Design develop IoT systems using Wi-Fi CC3200.
- Program the single board computers to read sensor data and posting in cloud.

Unit I
Architecture of the MSP430, Memory, Addressing modes, Reflections on the CPU instruction set. Clock system, Exceptions: Interrupts and resets. Functions and subroutines, Mixing C and assembly language, Interrupts, Interrupt service routines, Issues associated with interrupts, Lowpower modes of operation.

Unit II
ARM Cortex M4: Assembly language basics, Thumb-2 Technology, ARM Instruction set, Cortex M4 architecture, advantages, peripherals, instruction set, floating point operations, Advanced Cortex MX Microcontroller, core, architecture, on-chip wi-fi.

Unit III
GPIO, LCD display, graphical display, relays, Peripheral programming SPI, I2C, UART, Zigbee controller.
Sensors interfacing techniques- Port Programming, ADC, SPI thermometer, I2C thermometer, PWM generation and demodulation, DTH11, single wire thermometer, Frequency counters

Unit IV
ESP8266, NodeMCU, TI-CC3200, Access point and station point mode, HTTP, MQTT, transmission and receiving, Intel-Gallileo boards. Raspberry pi board, porting Raspbian, sensor interface examples, Python programming for cloud access, sensor systems using Arduino boards

Unit V
Interfacing and data logging with cloud: Thing speak, Things board, Blync platform

Textbooks
1. John H. Davies, "MSP430 Microcontroller Basics", 2011, 2nd ed., Newnes publishing, New York.
2. Jacob Fraden, "Hand Book of Modern Sensors: physics, Designs and Applications", 2014, 4th ed., Springer, New York.

References
1. Sergey Y. Yurish,"Digital Sensors and Sensor Systems: Practical Design", 2011, 1st ed., IFSA publishing, New York.
2. Jonathan W Valvano, "Introduction to ARM Cortex –M3 Microcontrollers", 2012, 5th ed., Create Space publishing, New York.
3. Muhammad Ali Mazidi, Shujen Chen, SarmadNaimi, SepehrNaimi, "TI ARM Peripherals Programming and Interfacing: Using C Language", 2015, 2nd ed., Mazidi and Naimi publishing, New York.

CSE572E	**IoT Communications and Networks**	Credits: 03 L T P 3 0 0

Course Outcomes
- Identify the IoT networking components with respect to OSI layer.
- Select IoT protocols and software.
- Comprehend the wireless technologies for Internet of Things.
- Understand the IoT architecture and building blocks for various domains.
- Understand basics of edge, fog and cloud computation architectures.

Unit I

Review of computer communication concepts (OSI layers, components, packet communication, Networks, TCP-IP, subnetting, IPV4 addressing and challenges). IPV6 addressing. IoT architecture References layer, Networking Basics of IoT, NFC, Wireless LAN.

Unit II

IoT Enabling Technologies: Communications, RFID and NFC (Near-Field Communication), Bluetooth Low Energy (BLE), LiFi, 6LowPAN, ZigBee, Z-Wave, LoRa, Protocols, HTTP, WebSocket, MQTT, CoAP, XMPP, Node-RED, Platforms, IBM Watson IoT—Bluemix, Eclipse IoT, AWS IoT.

Unit III

IoT Layered Architecture – 3-Layer, 4-Layer and 5-Layer architecture design, IoT Protocols and Softwares MQTT, UDP, MQTT brokers, publish subscribe modes, HTTP, COAP, XMPP IPv6, 6LoWPAN, RPL, and gateway protocols.

Unit IV

IoT MAC Fundamentals of MAC protocols Low duty cycle protocols and wakeup concepts, Contention Based protocols, Schedule-based protocols SMAC – BMAC, Traffic-adaptive medium access protocol (TRAMA), The IEEE 802.15.4 MAC protocol.

Unit V

Architecture of applications of IoT Architecture of IoT for Healthcare, Architecture of Smart cities, smart farming. Basics of cloud Computing-Need for clouds- concepts and models, Fog Computing Need for Fog computation, Fog data processing layers, Fog applications, Edge Computing Need for edge computation-Edge computing architectures.

Textbooks
1. Alessandro Bassi, Martin Bauer, Martin Fiedler, Thorsten Kramp, Rob van Kranenburg, Sebastian Lange, Stefan Meissner, "Enabling things to talk – Designing IoT solutions with the IoT Architecture References Model", Springer Open, 2016
2. Jan Holler, Vlasios Tsiatsis, Catherine Mulligan, Stamatis Karnouskos, Stefan Avesand, David Boyle, "From Machine to Machine to Internet of Things", Elsevier Publications, 2014.

References

1. Holger Karl, Andreas Willig, "Protocols and Architectures for Wireless Sensor Networks" 2011, 1 st ed., John Wiley & Sons, New Jersey.
2. S.-C. Hung et al.: Architecture Harmonization Between Cloud RANs and Fog Networks, IEEE Access: The Journal for rapid open access publishing, Vol.3, pp: 3019 – 3034, 2015.
3. Honbo Zhou, "The Internet of Things in the Cloud: A Middleware Perspective", CRC Press, 2012
4. Subhas Chandra Mukhopadhyay, Smart Sensing Technology for Agriculture and Environmental Monitoring, 2012, Springer, ISBN-10: 3642276377

CSE573E	**Software Architecture for IoT**	Credits: 03 L T P 3 0 0

Course Outcomes
- Understand IoT concepts: Students should gain a solid understanding of IoT fundamentals, including IoT architectures, protocols, communication paradigms, and device types.
- Design scalable IoT architectures: Students should be able to design scalable and flexible software architectures for IoT systems, considering factors such as device heterogeneity, data volume, network constraints, and security requirements.
- Select appropriate technologies: Students should learn how to evaluate and select appropriate technologies and platforms for building IoT solutions, such as cloud platforms, edge computing frameworks, communication protocols, and data storage solutions.
- Develop IoT applications: Students should be able to develop IoT applications using programming languages and frameworks suitable for IoT development, such as Python, Node.js, MQTT, CoAP, and others.
- Implement sensor data processing: Students should learn how to collect, process, and analyze sensor data from IoT devices, including techniques for data filtering, aggregation, normalization, and real-time processing.

Unit I

Overview of IoT ecosystem and architecture layers, Characteristics and requirements of IoT systems, Introduction to software architecture principles and patterns.
IoT Device Architecture - Design considerations for IoT devices, Power management and optimization strategies.

Unit II

Overview of IoT communication protocols (MQTT, CoAP, HTTP, etc.). Protocol selection criteria and trade-offs, implementation of IoT communication protocols.

Unit 3: Computing

Introduction to edge and fog computing concepts, Architectural patterns for edge/fog computing in IoT, Use cases and practical examples. Cloud-based IoT Architectures, Overview of cloud-based IoT platforms (AWS IoT, Azure IoT, Google Cloud IoT, etc.)., Designing scalable and secure cloud architectures for IoT, Integration with other cloud services (storage, analytics, etc.).

Unit IV

Threat modelling for IoT systems, Authentication, authorization, and access control mechanisms, Data encryption and secure communication protocols.

Unit V

Scalability patterns for IoT systems, Redundancy and fault tolerance strategies, Load balancing and resource management.

Textbooks:
1. ”Architecting the Internet of Things" by Dieter Uckelmann, Mark Harrison, Florian Michahelles.
2. "Building the Internet of Things: Implement New Business Models, Disrupt Competitors, Transform Your Industry" by Maciej Kranz.

References:
1. "Designing Connected Products: UX for the Consumer Internet of Things" by Claire Rowland, Elizabeth Goodman, Martin Charlier.
2. "Internet of Things for Architects: Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security" by Perry Lea.

CSE554E	**Embedded System Design**	Credits: 04 L T P 3 0 2

Course Outcomes
- The issues relating to hardware and software design concepts associated with processor in Embedded Systems.
- The concept of low power microcontrollers.
- The hardware software co- design issues pertaining to design of an Embedded System using low power microcontrollers

Unit I
An Embedded System-Definition, Embedded System Design and Development Life Cycle, An Introduction to Embedded system Architecture, The Embedded Systems Model, Embedded Hardware: The Embedded Board and the von Neumann Model, Embedded Processors: ISA Architecture Models, Internal Processor Design, Processor Performance, Board Memory: Read-Only Memory (ROM), Random-Access Memory (RAM), Auxiliary Memory, Memory Management of External Memory and Performance, Approaches to Embedded Systems, Small Microcontrollers, Anatomy of a Typical Small Microcontroller, Small Microcontrollers Memory, Embedded Software, Introduction to small microcontroller (MSP430).

Unit II
Architecture of the MSP430 Processor: Central Processing Unit, Addressing Modes, Constant Generator and Emulated Instructions, Instruction Set, Examples, Reflections on the CPU and Instruction Set, Resets, Clock System, Memory and Memory Organization.
Functions, Interrupts, and Low-Power Mode: Functions and Subroutines, Storage for Local Variables, Passing Parameters to a Subroutine and Returning a Result, Mixing C and Assembly Language, Interrupts, Interrupt Service Routines, Issues Associated with Interrupts, Low-Power Modes of Operation.

Unit III
Digital Input, Output, and Displays: Parallel Ports, Digital Inputs, Switch Debounce, Digital Outputs, Interface between Systems, Driving Heavier Loads, Liquid Crystal Displays, Simple Applications of the LCD.
Timers: Watchdog Timer, Timer_A, Timer_A Modes, Timer_B,Timer_B Modes, Setting the Real-Time Clock, State Machines.

Unit IV
Communication Peripherals in the MSP430, Serial Peripheral Interface, SPI with the USI, SPI with the
USCI, A Thermometer Using SPI Modes, Inter-integrated Circuit Bus(I²C) and its operations, State Machines for I²C Communication, A Thermometer Using I²C, Asynchronous Serial Communication, Asynchronous Communication with the USCI_A, A Software UART Using Timer_A, Other Types of Communication.

Unit V
Introduction to Code Composer studio (CC Studio Ver. 6.1) a tutorial, A Study of blinking LED, Enabling LED using Switches, UART Communication, LCD interfacing, Interrupts, Analog to Digital Conversion, General Purpose input and output ports, I2C.

TEXTBOOKS:
1. Tammy Noergaard "Embedded Systems Architecture: A Comprehensive Guide for Engineers and Programmers", Elsevier(Singapore) Pvt.Ltd.Publications, 2005.
2. John H. Davies "MSP430 Microcontroller Basics",Elsevier Ltd Publications, Copyright 2008.

REFERENCE BOOKS:
1. Manuel Jiménez Rogelio,PalomeraIsidoroCouvertier "Introduction to Embedded SystemsUsing Microcontrollers and the MSP430" Springer Publications, 2014.
2. Frank Vahid, Tony D. Givargis, "Embedded system Design: A Unified Hardware/Software Introduction", John Wily & Sons Inc.2002.
3. Peter Marwedel, "Embedded System Design", Science Publishers, 2007.
4. Arnold S Burger, "Embedded System Design", CMP Books, 2002.
5. Rajkamal, "Embedded Systems: Architecture, Programming and Design", TMH Publications,Second Edition, 2008.

CSE571E	**Architecting Smart IoT Devices**	Credits: 03 L T P 3 0 0

Course Outcomes

- Understanding of IoT Ecosystem: Students should gain a comprehensive understanding of the IoT ecosystem, including devices, sensors, connectivity protocols, cloud platforms, and applications.
- Architectural Design: Students should be able to design architectures for smart IoT devices considering various factors such as power consumption, data transmission, security, and scalability.
- Hardware Selection and Integration: Ability to select appropriate hardware components and integrate them into IoT devices based on the design requirements.
- Software Development: Proficiency in developing software for IoT devices, including firmware, embedded systems programming, and application development for device control and data processing.
- Connectivity Protocols: Understanding of various communication protocols used in IoT devices such as MQTT, CoAP, HTTP, and their suitability for different scenarios.
- Data Management and Analytics: Knowledge of techniques for managing and analyzing data generated by IoT devices, including data storage, processing, and visualization.

Unit I
Overview of smart IoT devices and their applications, Architectural components of IoT devices: sensors, actuators, microcontrollers, etc, Challenges and considerations in architecting IoT devices.

Unit II
Types of sensors and their characteristics, Interface protocols for sensor communication (I2C, SPI, UART, etc.), Data acquisition techniques and sensor fusion.

Unit III
Overview of IoT communication protocols (MQTT, CoAP, Bluetooth, LoRa, etc.), Selection criteria for communication protocols.

Unit IV
Power requirements and constraints in IoT devices, Low-power design techniques and optimization strategies, Energy harvesting and battery management.

Unit V
Threats and vulnerabilities in IoT devices, Authentication and encryption mechanisms, Secure boot, firmware updates, and OTA (Over-The-Air) updates.

Textbooks
1. " Internet of Things for Architects: Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security" by Perry Lea.
2. "Designing Connected Products: UX for the Consumer Internet of Things" by Claire Rowland, Elizabeth Goodman, Martin Charlier.

References
1. "IoT Developer's Handbook" by Artem Kuharenko
2. "IoT Security: A Practical Guide Book" by Raj Samani, Jim Reavis, Brian Honan.
3. "Low-Power Design Techniques and CAD Tools for Analog and RF Integrated Circuits" by Piet Wambacq, Georges Gielen.
4. "Battery Management Systems: Design by Modelling" by Gregory L. Plett.
5. "Practical Electronics for Inventors" by Paul Scherz, Simon Monk.

CSE556E	**Data Acquisition**	Credits: 04 L T P 3 0 2

Course Outcomes
- Elucidate the elements of data acquisition techniques.
- Design and simulate signal conditioning circuits.
- Explain various data transfer techniques
- Understand the components of Data Acquisition system

Unit I
Data Acquisition: Definition, Importance, and Applications, Components of Data Acquisition Types of Data Acquisition System, Signals used in Data Acquisition, Advantages and Disadvantages of Data Acquisition System.

Unit II
Analog and digital data acquisition, Sensor/Transducer interfacing, unipolar and bipolar
Transducers.

Unit III
Data Acquisition with Op-Amps: Operational Amplifiers, CMRR, Slew Rate, Gain, Bandwidth. Zero crossing detector,Peak detector, Window detector. Difference Amplifier, Instrumentation Amplifier AD 620,

Unit IV
Serial data transmission methods and standards RS 232-C: specifications connection and timing, 4-20 mA current loop, GPIB/IEEE-488, LAN, Universal serial bus, HART protocol.

Unit V
Single channel and multichannel, Graphical Interface (GUI) Software for DAS, RTUs, PC-Based data acquisition system.

Textbooks
1. Coughlin, R.F., Operational Amplifiers and Linear Integrated Circuits, Pearson Education (2006).
2. Kalsi, H.S., Electronic Instrumentation, Tata McGraw Hill (2002).
3. Murthy, D.V.S., Transducers and Instrumentation, Prentice Hall of India Private Limited (2006).

CSE557E	**IoT Programming and Big Data**	Credits: 04 L T P 3 0 2

Course Outcomes
- Understanding IoT ecosystem and analytics
- Identify Big Data and its Business Implications
- List the components of Hadoop and Hadoop Eco-System
- Access and Process Data on Distributed File System
- Manage Job Execution in Hadoop Environment
- To learn different concepts of multimedia communication.

Unit I
Introduction to IoT, applications, IoT architectures, introduction to analytics, IoT analytics challenges. IoT Devices and Networking Protocols: IoT devices, Networking basics

Unit II
Types of Digital Data, Introduction to Big Data, Big Data Analytics, History of Hadoop, Apache Hadoop, Analysing Data with Hadoop, Hadoop Streaming, Hadoop EcoSystem,

Unit III
The Design of HDFS, HDFS Concepts, Command Line Interface, Hadoop file system interfaces, Data flow.
Hadoop I/O: Compression, Serialization, Avro and File-Based Data structures.

Unit IV
Anatomy of a Map Reduce Job Run, Failures, Job Scheduling, Shuffle and Sort, Task Execution, Map Reduce Types and Formats, Map Reduce Features.

Unit V
Pig: Introduction to PIG, Execution Modes of Pig, Comparison of Pig with Databases, Grunt, Pig Latin, User Defined Functions, Data Processing operators

Textbooks:
1. Tom White " Hadoop: The Definitive Guide" Third Edit on, O'reily Media.
2. Seema Acharya, Subhasini Chellappan, "Big Data Analytics" Wiley.

References
1. Michael Berthold, David J. Hand, "Intelligent Data Analysis", Springer.
2. Jay Liebowitz, "Big Data and Business Analytics" Auerbach Publications, CRC press.

CSE605E	**Cloud Computing for IoT**	Credits: 04 L T P 3 0 2

Course Outcomes

- Understanding Cloud Computing: Students should grasp the fundamental concepts of cloud computing, including service models (SaaS, PaaS, IaaS), deployment models (public, private, hybrid, community clouds), virtualization, scalability, elasticity, and resource pooling.
- Understanding IoT: Students should comprehend the basic principles of the Internet of Things, including sensor technologies, connectivity protocols (such as MQTT, CoAP, HTTP), edge computing, IoT platforms, and applications in various domains.
- Integration of Cloud and IoT: Students should learn how to integrate IoT devices with cloud platforms, leveraging cloud services for data storage, processing, analytics, and visualization.
- Security and Privacy: Understanding security challenges in both cloud and IoT environments, including data privacy, authentication, authorization, encryption, secure communication, and mitigating risks associated with data breaches and cyber attacks.
- Scalability and Performance: Students should be able to design scalable and high-performance cloud-based IoT systems, considering factors like data volume, velocity, variety, and veracity.

Unit I

Cloud Computing: Definition, roots of cloud computing, characteristics, cloud architecture, deployment models, service models. Virtualization: Benefits & drawbacks of virtualization, server virtualization, virtualization of - operating system, platform, CPU, network, application, memory and I/O devices etc.

Unit II

Cloud Computing Service Platforms – Compute services, storage services, database services, application services, queuing services, e-mail services, notification services, media services, content delivery services, analytics services, deployment & management services, identity & access management services and their case studies. Security in cloud computing: issues, threats, data security and information security.

Unit III

Internet of Thing (IoT): Overview, conceptual framework, architecture, major components, common applications Design principles for connected devices: Modified OSI Model for IoT/M2M systems, wireless communication technologies - NFC, RFID, Bluetooth BR/EDR and Bluetooth low energy, ZigBee, WiFi, RF transceiver and RF modules. Data enrichment, data consolidation & device management at gateway.

Unit IV

Design principles for web connectivity: web communication protocols for connected devices: constrained application protocol, CoAP Client web connectivity, client authentication, lightweight M2M communication protocol. Message communication protocols for connected devices - CoAP-SMS, CoAP-MQ, MQTT, XMPP. IoT privacy, security and vulnerabilities and their solutions.

Unit V

Data Collection and Storage: Sensor data, time-series databases, NoSQL databases
Data Processing: Stream processing, batch processing, complex event processing
Data Analytics: Descriptive, diagnostic, predictive, prescriptive analytics for IoT data
IoT Device Programming: Embedded systems, firmware development
Cloud Application Development: Microservices, serverless computing, containerization
Integration with Cloud Services: APIs, SDKs, message brokers, event-driven architectures

Textbooks
1. "Building the Internet of Things: Implement New Business Models, Disrupt Competitors, Transform Your Industry" by Maciej Kranz.

References
1. "Cloud Computing: Concepts, Technology & Architecture" by Thomas Erl, et al.
2. "Cloud Computing and Internet of Things: A Survey" by Karim Djemame, et al.

CSE606E	**Programming Internet of Things**	Credits: 04 L T P 3 0 2

Course Outcomes
- Understand the fundamentals of IoT architecture and its components.
- Learn various sensors, actuators, and communication protocols used in IoT.
- Gain proficiency in programming languages and frameworks relevant to IoT development.
- Develop skills in designing, implementing, and deploying IoT applications.
- Explore real-world IoT applications and case studies.

Unit I

Introduction to IoT, Definition and scope of IoT, Evolution and trends in IoT, Applications and use cases, IoT Architecture, Sensor nodes, gateways, and cloud platforms, Communication protocols (MQTT, CoAP, HTTP, etc.), Data aggregation and processing

Unit II

Embedded Systems and Microcontrollers, Basics of embedded systems, Introduction to microcontrollers (Arduino, Raspberry Pi, ESP32, etc.), Interfacing sensors and actuators, Programming Languages for IoT, C/C++ for embedded systems, Python for IoT applications
JavaScript for web-based IoT applications

Unit III

IoT Development Frameworks and Platforms, Arduino IDE and libraries, Raspberry Pi development with Python, Node-RED for rapid IoT prototyping, IoT Security, Threats and vulnerabilities in IoT systems, Encryption and authentication mechanisms, Best practices for securing IoT devices and networks

Unit IV

IoT Data Analytics, Introduction to data analytics in IoT, Streaming data processing, Visualization and interpretation of IoT data, IoT Applications and Case Studies, Smart home automation, Industrial IoT (IIoT), Healthcare applications, Environmental monitoring

Unit V

IoT Application Development, Developing IoT Applications for Smart Home, Industrial IoT (IIoT) Applications, Healthcare IoT Applications, Agriculture IoT Applications, IoT Cloud Platforms, Introduction to IoT Cloud Platforms (AWS IoT, Azure IoT, Google Cloud IoT, etc.), Device Management and Connectivity, Cloud-based Analytics and Dashboards

Textbooks
1. "Building Arduino Projects for the Internet of Things" by Adeel Javed
2. "Python Programming for Arduino" by Pratik Desai
3. "Getting Started with IoT" by Cuno Pfister
4. "IoT Projects with Raspberry Pi" by John C. Shovic
5. "Hands-On IoT Solutions with Blockchain" by Maximiliano Santos and Enzo Calamo

CSE607E	**Artificial Intelligence of Things**	Credits: 04 L T P 3 0 2

Course Outcomes
- Understand the concepts, definitions, and significance of Artificial Intelligence of Things (AIoT), including its evolution and convergence of technologies.
- Explore AI techniques such as supervised, unsupervised, and reinforcement learning in the context of IoT.
- Learn about AIoT data acquisition from sensors and IoT devices, and preprocessing techniques for IoT data.
- Design AIoT systems, considering architectural aspects like edge, fog, and cloud computing, and integrating AI models with IoT platforms.
- Explore industry-specific AIoT applications, case studies, and ethical implications, and discuss future trends and advancements in AIoT research and development.

Unit I
Overview of AIoT: Concepts, definitions, and significance, Evolution of AI and IoT
Technologies and their convergence, Applications and use cases of AIoT in various domains,
Challenges and opportUnities in developing AIoT solutions.

Unit II
AI algorithms: Supervised, unsupervised, and reinforcement learning,- Machine learning models and techniques for IoT data analysis, Deep learning architectures: Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and their applications in IoT, Edge computing and AI inference at the IoT edge.

Unit III
Data sources: Sensors, actuators, and IoT devices, Data preprocessing techniques for IoT data,
Filtering, normalization, and feature extraction Time-series data analysis and forecasting for IoT applications, Anomaly detection and outlier identification in IoT datasets.

Unit IV
Architectural considerations for AIoT systems: Edge, fog, and cloud computing, Integration of
AI models with IoT platforms and frameworks, Real-time data processing and analytics in AIoT environments, Scalability, reliability, and performance optimization of AIoT solutions.

Unit V
Industry-specific AIoT applications: Smart manufacturing, healthcare, smart cities, etc. Case
studies of successful AIoT deployments and their impact, Ethical and societal implications of
AIoT technologies, Future trends and advancements in AIoT research and development.

Textbooks
1. "Internet of Things (IoT) Technologies for HealthCare: Third International Conference,
2. HealthyIoT 2016" Edited by Subhas Chandra Mukhopadhyay, Giovanni Saggio, Antonino Graziano, Athanasios Vasilakos

References
1. "Artificial Intelligence: A Guide to Intelligent Systems" by Michael Negnevitsky
2. "Hands-On Artificial Intelligence for IoT" by Amita Kapoor

CSE624E	**Software Defined Networks with IoT**	Credits: 03 L T P 3 0 0

Course Outcomes
1. Understand the principles behind the Modern Network approaches such as SDN NFV and IoT.
2. Ability to analyze Data Center topologies and virtualized environment
3. Understand the data traversal over virtualized environment for IoT
4. Design algorithms for virtualization over multi-tenant environments.

Unit I
Cloud Computing Internet of Things Types of Network and Internet Traffic Demand, Big Data, Cloud Computing, and Mobile Traffic Requirements: QoS and QoE Routing
Congestion Control

Unit II
Network Requirements The SDN Approach SDN- and NFV-Related Standards -SDN Data Plane OpenFlow Logical Network Device OpenFlow Protocol SDN,Control Plane Architecture REST API SDN Application Plane Architecture

Unit III
Background and Motivation for NFV Virtual Machines NFV Concepts NFV,References Architecture NFV Infrastructure Virtualized Network Functions NFV, Management and Orchestration NFV Use Cases SDN and NFV

Unit IV
The IoT Era Scope of the Internet of Things Components of IoT-Enabled Things -IoT World Forum References Model ITU-T, IoT References Model SDN and NFV over IoT Deployment

Unit V
Security Requirements SDN Security, NFV Security, IoT Security, IoT Security and Privacy Requirements Defined by ITU-T, IoT Security Framework.

Textbooks
1. William Stallings,"Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud" Publisher: Addison-Wesley 2015 ISBN: 9780134175393
2. Jim Doherty, "SDN and NFV Simplified: A Visual Guide to Understanding Software Defined Networks and Network Function Virtualization" 1st Edition

References
1. Paresh Shah, Syed Farrukh Hassan, Rajendra Chayapath, "Network Function virtualization with a touch of sdn"
2. Paul Goransson Chuck Black, "Software Defined Networks A Comprehensive Approach"

CSE621E	**IoT Security and Trust**	Credits: 03 L T P 3 0 0

Course Outcomes
- Understand the fundamentals of networks security, security architecture, threats and vulnerabilities in Internet of Things.
- Develop the ability to provide security to the cyber-physical systems components
- Develop the ability to conduct attacks on cyber-physical systems protocols and systems
- Develop the ability to design cyber-physical systems and architectures that preserves the privacy of the CPS components.

Unit I
Introduction, Defining Security and Privacy, Defining Cyber-Physical Systems, Approaches to Secure Cyber-Physical Systems, Threats, threat detection Ongoing Security and Privacy Challenges for CPS. Local Network Security for CPSs, Internet-Wide Secure Communication, Security and Privacy for Cloud-Interconnected CPSs

Unit II
Social Perspective and Motivation, Information Theoretic Privacy Measures, Privacy Models and Protection, National Security Concerns Arising from Cyber-Physical Systems, National Security Implications of Attacks on Cyber-Physical Systems, Threat modeling – Key elements. Identity management Models, Approaches using User-centric, Device-centric and Hybrid.

Unit III
Legal Considerations of Cyber-Physical Systems Privacy and Technology in Recent History, The Current State of Privacy Law, Meeting Future Challenges.
Key Management in CPS Introduction, Key Management Security Goals and Threat Model, CPS Key Management Design Principles, CPS Key Management, CPS Key Management Challenges and Open Research Issues.

Unit IV
Capability-based access control schemes, Concepts, identity-based and identity-driven, Lightweight cryptography, need and methods, IoT use cases, Cloud security, Digital identity management in cloud, Classical solutions, alternative solutions, Management of privacy and personal data in Cloud.

Unit V
Monitoring Systems, Privacy Protection for Cloud-Based Robotic Networks, Security Challenges and Applications, Vulnerability of CPS in Smart Cities, Data Security and Privacy in Cyber-Physical Systems for Healthcare.

Textbooks
1. John R. Vacca, "Computer and Information Security Handbook", Elsevier, 2013. Parikshit Narendra Mahalle , Poonam N. Railkar, "Identity Management for Internet of Things", River Publishers, 2015.
2. William Stallings, "Cryptography and Network security: Principles and Practice", 5th Edition, 2014, Pearson Education, India.
3. Houbing Song (Editor), Glenn A. Fink (Editor), Sabina Jeschke (Editor), "Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications" ISBN: 978-1-119-22607-9 October 2017 Wiley-IEEE Press

References
1. Christof Paar and Jan Pelzl, "Understanding Cryptography – A Textbook for Students and Practitioners", Springer, 2014.
2. Behrouz A.Forouzan : Cryptography & Network Security – The McGraw Hill Company,2007.
3. Charlie Kaufman, Radia Perlman, Mike Speciner, Network Security: "Private Communication in a public World", PTR Prentice Hall, Second Edition, 2002.
4. Alasdair Gilchrist, "IoT security Issues", Oreilly publications, 2017.
5. Suh, Sang C., et al., eds. Applied cyber-physical systems. Springer New York, 2014.
6. "Cybersecurity and Privacy in Cyber-Physical Systems, Yassine Maleh, Mohammad Shojafar, Ashraf Darwish, Abdelkrim Haqiq, 1st Edition, CRC Press, 2019"

CSE622E	**IoT Data Analytics**	Credits: 03 L T P 3 0 0

Course Outcomes
- Gain a general overview of data and analytics in the industry.
- To understand the meaning and significance of marketing analytics. Understand STP and apply analytics to it.
- Understanding Web Analytics and Google Analytics
- Understand the different types of reports in Google analytics and their usage.
- Perform analysis for performance of various social media efforts and Visualize data and communicate results

Unit I
Understanding data, Types of data - structured and unstructured. Introduction to the data ecosystem, Data analytics hierarchy - Data scientists vs engineers vs Business Analysts vs business managers.
Marketing analytics: Explain marketing analytics, Exploratory data analysis. Descriptive, predictive and prescriptive analytics, Analytics in segmentation, targeting and positioning

Unit II
Traditional web metrics and marketing decisions, Why analytics provides a better picture, Overview of web analytics KPIs and possible insights.
Introduction to Google Analytics, Working, setting up GA, Navigating the interface, Setting up different views with filters.

Unit III
Report snapshots and summary cards, real-time reports, overview reports, detail reports, compare data, filter data and customize reports, Explorations vs Reports, Sections: Canvas, variables and tab settings, Types of exploration: Path, funnel, user, segment, free-form, cohort and user lifetime, filters in explorations

Unit IV
Understanding Social Media Analytics - Twitter Analytics, YouTube Analytics, Describe the different types of data commonly found on social platforms. Understand the ethical sensitivities in obtaining and operating on social data. Use a social platform API to obtain data. Understand the structure of those data.

Unit V
Setting up social listening, Building audience cohorts, Segmenting audience based on various parameters (device/traffic source etc), Sentiment listening, Establishing KPIs, DM Campaign analysis. Effective data visualisation (GA Dashboard/Excel/Python), Building charts, graphs and tables for showcasing relevant insights

Textbooks:
1. Hemann, Chuck, and Ken Burbary. "Digital marketing analytics: Making sense of consumer data in a digital world". Pearson Education, 2013.
2. Kaushik, Avinash "Web analytics 2.0: The art of online accountability and science of customer centricity". John Wiley & Sons, 2009.
3. Sponder, Marshall "Social media analytics: Effective tools for building, interpreting, and using metrics". (2012).

CSE623E	**Advanced IoT Systems Integration and Industrial Applications**	Credits: 03 L T P 3 0 0

Course Outcomes
- Understanding role of edge computing in IoT.
- Understanding Role of cloud computing and security in IoT.
- Understanding the fusion of IoT with robotics and automation technologies
- Integration of machine learning with IoT

Unit I

Introduction to Edge Computing, Edge Devices and Gateway in IoT, Benefits and Challenges of Edge Computing, IoT Data Processing and Storage, Techniques for Analyzing IoT Data, Data-Driven Decision-Making in Industrial Applications

Unit II

Overview of Cloud Service Models, Cloud Service Providers Evaluation Toolkit, Scalability and Resource Management in Cloud-Based IoT, Cloud-Based Data Integration, Cloud Cost Optimization Strategies

Unit III

Security Risks in IoT Systems, Privacy Concerns in IoT Applications, Security Measures for IoT Devices and Networks, Overview of IoT Regulations and Standards, Role of Compliance in IoT Security and Privacy.

Unit IV

Integration of IoT with Robotics and Automation Technologies, IoT-Enabled Robots and Cobots, Benefits and Challenges of IoT-Driven Automation, Strategies for IoT and Robotics Integration, Assessing the Impact of IoT-Driven Automation, Designing a Comprehensive IoT Solution with Robotics and Automation Technologies.

Unit V

Introduction to machine learning, Types- supervised, unsupervised, reinforcement, semi-supervised learning, features and feature selection techniques, bias and variance tradeoff, overfitting and under fitting, machine learning for mobile devices. CASE STUDIES/INDUSTRIAL APPLICATIONS: IoT applications in home, infrastructures, buildings, security, Industries, Home appliances, other IoT electronic equipments, Industry 4.0 concepts

Textbooks:
1. IoT Fundamentals: Networking Technologies, Protocols and Use Cases for Internet of Things, David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Rob Barton and Jerome Henry, Cisco Press, 2017
2. Internet of Things – A hands-on approach, Arshdeep Bahga, Vijay Madisetti, Universities Press, 2015

References
1. The Internet of Things – Key applications and Protocols, Olivier Hersent, DavidBoswarthick, Omar Elloumi and Wiley.
2. "From Machine-to-Machine to the Internet of Things – Introduction to a New Age of Intelligence",Jan Ho¨ ller, VlasiosTsiatsis, Catherine Mulligan, Stamatis, Karnouskos, Stefan Avesand. David Boyle and Elsevier.

CSE608E	**IoT Applications and Web Development**	Credits: 04 L T P 3 0 2

Course Outcomes
- Understand web technologies including HTML, CSS, and JavaScript fundamentals.
- Explore Internet of Things (IoT) concepts, sensors, actuators, and communication protocols.
- Learn embedded programming for IoT devices and connecting them with web applications.
- Gain knowledge of Node.js and Express for server-side development and building web applications.
- Implement MongoDB for NoSQL database operations and build RESTful APIs with Node.js, Express, and MongoDB.

Unit I
Introduction to web technologies, HTML fundamentals: structure, elements, tags, and attributes, CSS basics, selectors, properties, styling, and layout techniques, JavaScript variables, data types, operators, and control structures, Document Object Model (DOM),JSON (JavaScript Object Notation)

Unit II
Concepts, definitions, and significance, Sensors, actuators, and embedded systems, Data collection, processing, and storage in IoT systems, Wireless communication standards, IoT communication protocols.

Unit III
Introduction to embedded systems and IoT devices, Connecting web applications with IoT devices using APIs, Implementing basic IoT functionalities, jQuery library for DOM manipulation and event handling, front-end frameworks like Bootstrap for responsive design.

Unit IV
Overview of server-side JavaScript with Node.js, Setting up a server using Node.js and handling HTTP requests, Express.js framework for building web applications, Routing, middleware, and request handling in Express

Unit V
Introduction to NoSQL databases and MongoDB, CRUD operations with MongoDB: creating, reading, updating, and deleting data, Building RESTful APIs with Node.js, Express, and MongoDB, Implementing data validation and error handling in RESTful APIs

Textbooks
1. The "Internet of Things" by Samuel Greengard
2. The "Pragmatic Programmer" by Andrew Hunt and David Thomas

References
1. "Precision: Principles, Practices and Solutions for the Internet of Things" by Timothy Chou

VERTICAL III:
ARTIFICIAL INTELLIGENCE AND
MACHINE LEARNING

CSE559E	**Data Warehousing and Data Mining**	Credits: 04 L T P 3 0 2

Course Outcomes
- Understand the principles of data warehousing and data mining.
- Design and implement data warehouse architectures for efficient data storage and retrieval.
- Master data mining algorithms for classification, clustering, association, and sequence mining.
- Apply preprocessing, querying, and visualization techniques to real-world datasets.
- Develop practical skills through hands-on projects using industry-standard tools.

Unit I: Introduction
Data Warehousing: Concepts, Architecture (Enterprise, Data Marts), Components. Data Mining: Definition, KDD Process, Applications. Key Differences: OLTP vs. OLAP, Data Mining vs. Machine Learning. Data Characteristics: Structured, Semi-structured, Unstructured data; Statistical descriptions; Data visualization; Data similarity and dissimilarity.

Unit II: Data Warehouse Design, OLAP, and Data Preprocessing
Schemas: Star, Snowflake, Fact Constellation. Modeling: Multidimensional Models; ROLAP, MOLAP, HOLAP. OLAP Operations: Roll-up, Drill-down, Slice, Dice, Pivot. ETL Process: Extraction, Transformation, Loading; Data cube technology; Trends in Distributed Warehousing.
Data Preprocessing: Cleaning, Integration, Transformation, Discretization, Reduction. Feature Engineering: Selection and Dimensionality Reduction (PCA, LDA).

Unit III: Classification
Algorithms: Decision Trees (C4.5, CART), Naive Bayes, Support Vector Machines (SVMs), Lazy Learners (k-NN). Neural Networks: Classification by Backpropagation. Advanced Methods: Ensemble methods, Classification Using Frequent Patterns. Evaluation: Metrics for evaluating classifier performance.

Unit IV: Frequent Pattern Mining, Association Mining and Clustering
Algorithms: Apriori, FP-Growth, ECLAT. Concepts: Closed patterns, Maximal patterns, Correlation analysis; Applications: Market Basket Analysis, Recommendation Systems.
Clustering Techniques: Partitioning Methods (k-Means), Hierarchical methods, Density-based methods, Grid-based methods, Probabilistic model-based methods, Evaluation of Clustering.

Unit V: Advanced Topics in Data Mining
Sequence and Time-Series Mining: GSP, PrefixSpan, Trend Analysis; Text Mining: Tokenization, TF-IDF, Sentiment Analysis; Web Mining: Content, Structure, and Usage Mining; Big Data Mining Basics: Hadoop, Apache Spark, Scalable Algorithms.

List of Practicals

1. Load a dataset (e.g. UCI Iris or Kaggle Retail dataset), analyze its structure (structured/unstructured), and generate summary statistics (mean, median, missing values). Tools: Python (Pandas, NumPy).

2. Create a star schema for a retail dataset with fact (sales) and dimension tables (customer, product, time). Implement it using SQL.

3. Using the star schema from Practical 2, perform OLAP operations (roll-up, drill-down, slice, dice) to analyze sales by region and time. Use SQL, Tableau (for visualization).

4. Clean a dataset (e.g., handle missing values, normalize data, remove outliers) and reduce dimensionality using PCA. Tools: Python (Pandas, Scikit-learn), Dataset: UCI Adult Income or Kaggle Titanic.

5. Implement the Apriori algorithm to find frequent itemsets and association rules (e.g., market basket analysis). Tools: Python (mlxtend library), Dataset: Kaggle Grocery Store Dataset or UCI Market Basket.

6. Build a decision tree classifier (C4.5 or CART) on a labeled dataset and evaluate using accuracy, precision, recall, and F1-score. Tools: Python (Scikit-learn), Dataset: UCI Breast Cancer or Kaggle Credit Risk.

7. Load a small, labeled dataset for classification, preprocess the data (handle missing values, scale features), implement a *k*-NN classifier and experiment with the number of neighbors (*k*), evaluate the model using accuracy, precision, and recall, and visualize the results with a confusion matrix. Tools: Python (Scikit-learn, Pandas, Matplotlib), Dataset: UCI Iris Dataset.

8. Implement *k*-Means and DBSCAN on a dataset, compare results using silhouette score, and visualize clusters. Tools: Python (Scikit-learn, Matplotlib), Dataset: UCI Mall Customers or Kaggle Customer Segmentation.

9. Preprocess a text dataset (tokenization, stop-word removal, TF-IDF) and perform sentiment analysis using a classifier. Tools: Python (NLTK, SpaCy, Scikit-learn), Dataset: Kaggle Twitter Sentiment or UCI Movie Reviews.

10. Implement a clustering or classification algorithm (e.g., *k*-Means or logistic regression) on a large dataset using Apache Spark. Tools: Apache Spark (PySpark), Python, Dataset: Kaggle Big Data Dataset (e.g., NYC Taxi Trips).

Textbook
1. Han J, Pei J, and Tong H. Data mining: concepts and techniques. Morgan Kaufmann; 2022

References
1. Tan PN, Steinbach M, and Kumar V. Introduction to data mining. Pearson Education India: 2016.
2. Leskovec J, Rajaraman A, Ullman JD. Mining of massive data sets. Cambridge University press; 2020.
3. Mitchell TM, Mitchell TM. Machine learning. New York: McGraw-Hill; 1997.
4. KimballR, Ross M. The data warehouse toolkit: The definitive guide to dimensional modeling.
2. John Wiley & Sons; 2013.
5. Jarke M, Lenzerini M, Vassiliou Y, Vassiliadis P. Fundamentals of data warehouses.
3. Springer Science & Business Media; 2013.

Online Resources:
1. https://hanj.cs.illinois.edu/bk3/bk3 slidesindex.htm
2. https:/web.stanford.edu/class/cs246/

CSE574E	**Soft Computing**	Credits: 03 L T P 3 0 0

Course Outcomes
- Know about the concepts of fuzzy logic, crisp logic, fuzzy relation, fuzzy implication rule
- Know about the concepts of optimization theory genetic computing, and evolutionary computing.
- Know about the concepts of classifications, Implementation, and training
- Know about the concept of hybrid systems, like neuro-fuzzy systems, fuzzy genetic systems, and particle intelligence.

Unit I
What is Soft Computing, soft computing vs. hard computing, soft computing paradigms, and applications of soft computing. Basics of Machine Learning. Dealing with Imprecision and Uncertainty- Probabilistic Reasoning. Optimization: Derivative-based Optimization – Descent Methods

Unit II
Basics of Neural Networks- Neural Network Structure and Function of a single neuron: Biological neuron, artificial neuron, McCulloch Pitt model, different activation functions, Supervised Learning algorithms- Perceptron (Single Layer, Multi layer), Linear separability, ADALINE, MADALINE, RBF networks , Widrow Hoff, learning rule, Delta learning rule, Back Propagation algorithm, Un-Supervised Learning algorithms- Hebbian Learning, , Self Organizing Maps.

Unit III
Fuzzy set theory, Fuzzy set versus crisp set, Crisp relation & fuzzy relations, Fuzzy systems: crisp logic, fuzzy logic, introduction & features of membership functions, Fuzzy rule base system: fuzzy propositions, formation, decomposition & aggregation of fuzzy rules, fuzzy reasoning, fuzzy inference systems, Mamdani Fuzzy Models –
Sugeno Fuzzy Models, Adaptive Neuro-Fuzzy Inference Systems Architecture

Unit IV
Genetic algorithm Fundamentals, basic concepts, working principle, encoding, fitness function, reproduction, Genetic modeling: Inheritance operator, cross over, mutation operator, Generational Cycle, Convergence of GA, Applications & advances in GA, Differences & similarities between GA & other traditional methods.

Unit V
Evolutionary Computing: Genetic programming (GP), Ant colony optimization (ACO), Particle swarm optimization (PSO), Artificial Immune System (AIS).

References
1. S, Rajasekaran & G.A. Vijayalakshmi Pai, "Neural Networks, Fuzzy Logic & Genetic Algorithms, Synthesis & applications", PHI Publication.
2. S.N. Sivanandam& S.N. Deepa, "Principles of Soft Computing", Wiley Publications.
3. Jyh-Shing Roger Jang, Chuen-Tsai Sun, EijiMizutani, "Neuro-Fuzzy and Soft Computing", Prentice-Hall of India.
4. S Andries P Engelbrecht, Computational Intelligence: An Introduction, Wiley Publications.

CSE561E	**Distributed Machine Learning**	Credits: 04 L T P 3 0 2

Course Outcomes
- Understanding the fundamentals of parallel and distributed platforms, including hardware models, software frameworks, and application considerations.
- Gaining knowledge of Distributed Machine Learning (DML) platforms and scalability-motivated DML approaches.
- Learning about privacy-motivated DML, including privacy-preserving techniques and schemes.
- Mastering various distributed machine learning algorithms and understanding their implementation in frameworks like Apache Spark MLlib, TensorFlow, PyTorch, and others.
- Exploring the architecture and ecosystem of distributed machine learning, including its benefits and challenges.
- Gaining practical experience with cloud platforms supporting distributed machine learning, such as AWS, Microsoft Azure, and Google Cloud.
- Studying threaded and GPU-based formulations, multi-GPU formulations, and the impact on data convergence and accuracy.

Unit I
Basics of Parallel and Distributed Platforms Hardware models, Software frameworks, Application considerations (data distribution, real-time constraints, resource constraints), Distributed Machine Learning (DML), DML Platforms, Scalability-Motivated DML, Large-Scale Machine Learning, Scalability-Oriented DML Schemes, Privacy-Motivated DML, Privacy Preserving Techniques, Privacy-Preserving DML Schemes, Privacy-Preserving Gradient Descent, Vanilla Federated Learning.

Unit II
Distributed Machine Learning Algorithms Parameter server, AllReduce, MapReduce, Stochastic gradient descent (SGD), Alternating least squares (ALS), Distributed Machine Learning Frameworks Apache Spark MLlib, TensorFlow, PyTorch, Horovod, Apache Mahou, H2O.ai.

Unit III
A References architecture for distributed machine learning, distributed machine learning ecosystem, benefits for Distributed Machine Learning, Challenges for Distributed Machine Learning

Unit IV
Cloud Platforms for Distributed Machine Learning Amazon Web Services (AWS) Sagemaker, Microsoft Azure Machine Learning, Google Cloud Machine Learning Services, Databricks, Distributed Machine Learning using MLlib with Spark.

Unit V
Algorithms for threaded and GPU-based formulations, Multi-GPU formulations, scaleout, Data, convergence, and accuracy, Important applications of different learning formulations in parallel and distributed environments.

Textbooks
1. "Distributed Systems: Principles and Paradigms" by Andrew S. Tanenbaum and Maarten Van Steen
2. "Distributed Machine Learning: Foundations, Algorithms, and Systems" by Qirong Ho, Garth Gibson, and Joseph Gonzalez
3. "TensorFlow for Machine Intelligence" by Sam Abrahams, Danijar Hafner, Erik Erwitt, and Ariel Scarpinelli
4. "Mastering Machine Learning on Google Cloud Platform: Implement machine learning models in GCP and build smarter web services" by Giuseppe Ciaburro and V Kishore Ayyadevara

CSE575E	**Cloud Computing for Machine Learning**	Credits: 03 L T P 3 0 0

Course Outcomes
- Understand the principles of cloud computing systems, including different architectures and service models, and apply this knowledge to design and deploy cloud-based solutions effectively.
- Analyze and apply various machine learning algorithms, including supervised and unsupervised methods such as regression, classification, clustering, and dimensionality reduction, to solve real-world problems.
- Develop proficiency in the machine learning life cycle, from data storage and cleaning to model training, testing, deployment, and monitoring, ensuring the robustness and effectiveness of machine learning solutions.
- Gain hands-on experience in cloud programming with Spark, including working with resilient distributed datasets (RDD) and utilizing Spark MLlib for scalable machine learning tasks.
- Acquire practical skills in TensorFlow for deep learning model development, including tensor manipulation, variable declaration, and implementation of loss functions, enabling effective batch training and model optimization.
- Explore MLOps practices and tools, including cloud-based machine learning frameworks such as Azure HDInsight, Spark MLlib, and Amazon Machine Learning Platform, and apply them to solve real-world problems, with a focus on healthcare applications.

Unit I
Principles of cloud computing systems, cloud architectures, service models; Cloud architectures and service platform: cloud architecture and infrastructure design, dynamic deployment, various cloud service examples;

Unit II
Taxonomy of Machine Learning Methods. Supervised Regression and Classification Methods (Linear Regression for Prediction or Forecasting, Decision Trees for Machine Learning, Bayesian Classifier, Support Vector Machines). Unsupervised Machine Learning Algorithms (Association Analysis, Clustering Methods, Dimensionality Reduction). Clustering and Dimensionality Reduction Methods, Reinforcement Learning, and Semi-Supervised Learning Methods. Model Development and Selection for Machine Learning (Model Over- and Under-fitting)

Unit III
Data storage, data cleaning, data transformation, model training, model testing, model deployment and integration, model monitoring and feedback;
Cloud Programming with Spark: understanding resilent distributed dataset (RDD), Spark MLlib;

Unit IV
Declaring tensors, place holders and variables, working with matrices, declaring operations, data sources, implementing loss functions, batch training.

Unit V
Cloud-Based Machine Learning Frameworks (e.g., Azure HDInsight and Data Lake; Spark MLlib for Machine Learning and GraphX for Graph Processing; Azure Machine Learning Workspace; Amazon Machine Learning Platform) Example: Healthcare Problems and Machine Learning Related Applications

Textbooks
1. K. Hwang, Cloud Computing for Machine Learning and Cognitive Applications, MIT Press, 2017.
2. R.O. Duda, P.E. Hart and D.G. Strok, Pattern Classification, 2nd Edn., John Wiley & Sons Pvt. Ltd, 2001.

References
1. M.R. Karim and M.M. Kaysar, Large Scale Machine Learning with Spark, Packt Publishing, 2016.
2. N. McClure, TensorFlow Machine Learning Cookbook, Packt Publishing Limited, 2017.

CSE558E	**Deep Learning**	Credits: 04 L T P 3 0 2

Course Outcomes
- Recognize the characteristics of deep learning models and their applicability to real-world problems.
- Understand and implement key deep learning architectures using Python-based libraries.
- Select and apply appropriate deep learning techniques for various types of data (text, image, sequential).
- Design, build, train, and validate deep learning models in a hands-on environment.
- Evaluate the performance of deep neural networks and apply model optimization techniques.
- Experiment with advanced architectures such as CNNs, RNNs, Autoencoders, and GANs through lab exercises.
- Design the test procedures to assess the efficacy of the developed model.

Unit I: Foundations of Deep Learning
Learning algorithms, Maximum likelihood estimation, Building machine learning algorithms, Neural Networks Multilayer Perceptron, Back-propagation algorithm and its variants stochastic gradient Decent, Curse of Dimensionality.
Lab Focus:
Implement perceptron and MLP from scratch using NumPy, Visualization of loss surface and training dynamics, Hands-on gradient descent variants

Unit II: Representation Learning & Unsupervised DL
Machine Learning vs Deep Learning, Representation Learning, Network width/depth, Activation Functions: RELU, LRELU, ERELU, Unsupervised Training of Neural Networks, Restricted Boltzmann Machines, Auto Encoders, Deep Learning Applications
Lab Focus:
Train and visualize different activation functions, Build Autoencoders and RBMs using PyTorch/Keras, Feature extraction using unsupervised learning

Unit III: Convolutional Neural Networks (CNN)
CNN architecture, layers, filters, Parameter sharing and regularization, ResNet, AlexNet architectures
Lab Focus:
Train CNN models on MNIST/CIFAR-10, Implement custom CNN layer stacks, Fine-tune pre-trained ResNet/AlexNet

Unit IV: Sequence Models
Recurrent Neural Networks (RNN), Bi-RNN, Sequence-to-sequence models, Backpropagation Through Time (BPTT), LSTM and GRU, Transfer Learning Techniques
Lab Focus:
Implement simple RNN, LSTM using Keras, Sentiment analysis using RNN/LSTM, Translation task with encoder-decoder architecture

Unit V: Generative Models
Variants of Autoencoders: Under complete Autoencoder, Regularized Autoencoder, stochastic Encoders, and Decoders, Contractive Encoders, Deep Belief Networks, Boltzmann Machines, Generative Adversarial Networks (GANs)
Lab Focus:
Train undercomplete, denoising, and variational autoencoders, Implement basic GAN to generate handwritten digits, Experiment with DCGAN for image synthesis

List of Practicals

Each lab should include implementation, training, visualization, and report submission.

1. Implementing Perceptron and MLP using NumPy

2. Exploring Activation Functions and Their Gradients

3. Backpropagation and Optimizers (SGD, Adam, RMSprop)

4. Training Feedforward Neural Networks on MNIST

5. Autoencoders – Construction and Denoising

6. Restricted Boltzmann Machines – Hands-on Training

7. Convolutional Neural Networks with TensorFlow/Keras

8. Transfer Learning with Pre-trained ResNet/AlexNet

9. Recurrent Neural Networks and LSTM for Sequence Data

10. Sequence-to-Sequence Model for Translation Task

11. Implementing Variational Autoencoders

12. Basic GAN and DCGAN Image Generation

13. Model Evaluation Techniques (Accuracy, Precision, Recall, F1, ROC)

14. Project Work: Choose a Dataset and Build Full DL Pipeline

Textbooks
1. Ian Goodfellow, YoshuaBengio and Aaron Courville, "Deep Learning", MIT Press, 2017.
2. Josh Patterson, Adam Gibson "Deep Learning: A Practitioner's Approach", O'Reilly Media,2017
3. Umberto Michelucci "Applied Deep Learning. A Case-based Approach to Understanding Deep Neural Networks" Apress, 2018.

References
1. Kevin P. Murphy "Machine Learning: A Probabilistic Perspective", The MIT Press, 2012.
2. EthemAlpaydin,"Introduction to Machine Learning", MIT Press, Prentice Hall of India, Third Edition 2014.
3. Giancarlo Zaccone, Md. RezaulKarim, Ahmed Menshawy "Deep Learning with TensorFlow:
4. Explore neural networks with Python", Packt Publisher, 2017.
5. Antonio Gulli, Sujit Pal "Deep Learning with Keras", Packt Publishers, 2017.
6. Francois Chollet "Deep Learning with Python", Manning Publications, 2017.

CSE560E	**Natural Language Processing**	Credits: 04 L T P 3 0 2

Course Outcomes
- Practice and learn the computational properties of natural languages and the commonly used algorithms for processing linguistic information
- Demonstrate proficiency in various text representation techniques, including one-hot encoding, bag-of-words, TF-IDF, and the Vector Space Models.
- Able to design models and solve the real-world challenges
- Learn the concept behind natural language processing and able to extract information from text and verbal data
- Understanding semantics and pragmatics of English language for processing

Unit I
History of NLP, Generic NLP System, Levels of NLP, Knowledge in Language Processing, Ambiguity in Natural Language, NLP Stages, NLP Challenges, NLP Applications: Machine Translation, Information Retrieval, Question Answers System, Categorization, Summarization, Sentiment Analysis, Named Entity Recognition

Unit II
Language Modelling and Text Representation: N-Gram, N-Gram Probability Estimation, Evaluation of Language Model, Smoothing Techniques: Laplace, Good Turing, Kneser-Ney, Text Representation: One Hot Encoding, Bag-of-Word, TF-IDF, Vector Space Model, Latent Semantic Analysis Word Embedding Word2Vec, Glove, fastText.

Unit III
Word Level Analysis: Morphology Analysis –Survey of English Morphology, Inflectional Morphology & Derivational Morphology, Part-of-Speech (POS) Tagging - Tag Set for English (Penn Treebank), Rule-based POS Tagging, Stochastic POS Tagging, Hidden Markov Model

Unit IV
Syntactic and Semantic Analysis: Introduction, Context-Free Grammar, Parsing, Probabilistic Parsing Meaning Representation, Semantic Analysis: Lexical Semantics, Word Sense Disambiguation, Attachment for Fragment of English-Sentences, Noun Phrases, Verb Phrases, Prepositional Phrases, Relations Among Lexemes & And Their Senses – Homonymy, Polysemy, Synonymy, Hyponymy.

Unit V
Pragmatics: Discourse – References Resolution, References Phenomenon, Syntactic and Semantic Constraints on Co-References, Co-References Resolution, Text Coherence. Machine Translation, Transfer Metaphor, Interlingua and Statistical Approaches.

List of Practicals

1. Text Preprocessing: Tokenize, remove stopwords, and lemmatize text using NLTK/spaCy. Clean raw input for downstream tasks.

2. N-Gram Model: Build bigram/trigram models with NLTK. Compute probabilities and apply Laplace smoothing for unseen words.

3. BoW & TF-IDF: Convert text to vectors using CountVectorizer (BoW) and TfidfVectorizer. Compare outputs for sample sentences.

4. Word2Vec/GloVe: Train embeddings with gensim, find similar words (e.g., "king → queen"), and visualize via PCA.

5. POS Tagging: Tag words using NLTK's Penn Treebank or spaCy. Compare rule-based and stochastic (HMM) approaches.

6. Named Entity Recognition: Extract entities (Person, Org) with spaCy's NER. Visualize using displacy.

7. Sentiment Analysis: Analyze polarity with TextBlob or train Naive Bayes on IMDb reviews.

8. Syntactic Parsing Parse sentences with NLTK's CFG and spaCy's dependency parser. Draw tree structures.

9. Word Sense Disambiguation: Resolve ambiguous words using NLTK's Lesk algorithm.

Textbooks
1. Daniel Jurafsky, James H Martin, "Speech and Language Processing: An introduction to Natural Language Processing, Computational Linguistics and Speech Recognition", 2/e, Prentice Hall, 2008.
2. C. Manning, H. Schutze, "Foundations of Statistical Natural Language Processing", MIT
3. Steven Bird, Ewan Klein, Edward Loper, "Natural Language Processing in Python", O'Reilly.

CSE576E	**Bioinformatics and Computational Biology**	Credits: 03 L T P 3 0 0

Course Outcomes
- Establish foundational knowledge in DNA analysis and protein structure-function relationships, exploring sequence alignment and database utilization.
- Master techniques for DNA sequence analysis and protein structure understanding, including secondary structure prediction and sequence alignment.
- Acquire proficiency in analyzing protein sequences and tertiary structures, utilizing visualization tools and structural classification methods.
- Investigate protein stability and folding rates, understanding energetic contributions and the significance of binding site residues.
- Explore computer-aided drug design and algorithm development, utilizing molecular docking, QSAR modeling, and machine learning techniques for bioinformatics applications.

Unit I
Introduction, DNA sequence analysis, DNA Databases, Protein structure and function, protein sequence databases, sequence alignment, PAM matrix, Global and local alignment, BLAST: features and scores

Unit II
Multiple sequence alignment, Conservation score, phylogenetic trees, Protein sequence analysis, hydrophobicity profiles, non-redundant datasets, Protein secondary structures, Ramachandran plot, propensity, secondary structure prediction

Unit III
Protein tertiary structure, Protein Data Bank, visualization tools, structural classification, Protein structural analysis, protein structure prediction

Unit IV
Protein stability, energetic contributions, database, stabilizing residues, Protein folding rates, proteins interactions, binding site residues

Unit V
Computer aided drug design, docking, screening, QSAR, Development of algorithms, awk programming, machine learning techniques, applications using WEKA

Textbooks
1. M. Michael Gromiha, Protein Bioinformatics: From Sequence to Function, Academic Press, 2010
2. D.E. Krane and M.L. Raymer, Fundamental concepts of bioinformatics, Pearson Education Inc. 2006

CSE610E	**Computer Vision**	Credits: 04 L T P 3 0 2

Course Outcomes
- Implement key image processing and computer vision techniques using OpenCV and Python.
- Analyze shapes, contours, and object features in 2D and 3D images.
- Apply object detection and boundary tracking methods with real-time visualization.
- Implement region and boundary descriptors including chain codes and moments.
- Use Hough Transform and its variants for geometric shape detection.
- Understand and simulate 3D vision techniques including triangulation and reconstruction.
- Apply motion tracking algorithms using real-time video data.
- Develop practical computer vision applications such as surveillance and driver-assistance systems.

Unit I: Image Processing Fundamentals
Classical filtering operations, Thresholding techniques, Edge, corner, and interest point detection, Morphological operations and texture analysis
Lab Focus:
Implement smoothing, sharpening, edge detection using OpenCV, Harris corner detection, SIFT/SURF simulation, Morphological operations and texture-based segmentation

Unit II: Shape Analysis & Descriptors
Binary shape analysis, labeling, counting, size filtering, distance functions Skeletonization, thinning, Boundary tracking, active contours, shape models and shape recognition, centroidal profiles, handling occlusion, boundary length measures, Descriptors: chain codes, Fourier, region-based (moments)
Lab Focus:
Contour detection and labeling using OpenCV, Shape descriptors visualization (chain codes, Hu moments), Active contour simulation and shape matching

Unit III: Hough Transform and Shape Detection
Line, circle, and ellipse detection using HT and RANSAC, Generalized Hough Transform (GHT), spatial matched filtering – GHT for ellipse detection, Case study: Human iris location-hole detection
Lab Focus:
Line detection using Hough Transform, Circle and ellipse detection projects, GHT for custom object templates

Unit IV: 3D Vision and Motion Estimation
Projection models, photometric stereo, shape from texture – shape from focus – active range finding – surface representations – point-based representation – volumetric representations, 3D object recognition and reconstruction, Introduction to motion, triangulation, bundle adjustment, translational alignment, parametric motion, spline-based motion, optical flow, layered motion
Lab Focus:
Depth map estimation from stereo images, Triangulation and motion estimation, Dense optical flow visualization using Farneback/Lucas-Kanade methods

Unit V: Real-World Applications
Face detection/recognition (Eigenfaces, 3D models), Active appearance and 3D shape models of faces; Surveillance: background subtraction, occlusion handling; In-vehicle systems: road marking, sign detection, pedestrian tracking
Lab Focus:
Face detection using Haar cascades/DLIB, Background subtraction and motion tracking using Kalman/particle filters, Road sign and lane detection using edge maps and CNN-based classifiers

List of Practicals

Each lab involves coding, analysis, testing on datasets/videos, and performance evaluation.

1 Introduction to OpenCV and image I/O operations

2 Filtering (Gaussian, Median) and Thresholding Techniques

3 Edge Detection (Sobel, Canny) and Morphological Operations

4 Corner and Keypoint Detection (Harris, FAST, ORB)

5 Binary Shape Analysis and Object Labeling

6   Skeletonization and Contour Tracking

7   Chain Codes, Hu Moments, Fourier Descriptors

8   Hough Transform for Line, Circle, and Ellipse Detection

9   Generalized Hough Transform for Custom Shapes

10 Stereo Vision and Disparity Mapping

11 Motion Detection with Optical Flow

12 Face Detection and Recognition (Eigenfaces/Deep Learning)

13 Background Subtraction and Tracking

14 Final Mini Project – End-to-End Application (e.g., Smart Surveillance or Road Detection System)

Textbooks

1. D. L. Baggio et al., "Mastering OpenCV with Practical Computer Vision Projects", Packt Publishing, 2012.
2. E. R. Davies, "Computer & Machine Vision", Fourth Edition, Academic Press, 2012.
3. Jan Erik Solem, "Programming Computer Vision with Python: Tools and algorithms for analyzing images", O'Reilly Media, 2012.
4. Mark Nixon and Alberto S. Aquado, "Feature Extraction & Image Processing for Computer Vision", Third Edition, Academic Press, 2012.
5. R. Szeliski, "Computer Vision: Algorithms and Applications", Springer 2011.
   Simon J. D. Prince, "Computer Vision: Models, Learning, and Inference", Cambridge University Press, 2012.

CSE628E	**Quantum Machine Learning**	Credits: 03 L T P 3 0 0

Course Outcomes
- To learn and understand basics of quantum mechanics and computing
- Ability to design and analyze quantum circuits using an array of quantum gates and operators, understanding their application in quantum computing.
- Learn various quantum data encoding techniques and apply fundamental quantum algorithms to manipulate and store data on quantum computers.
- Hands-on experience in implementing quantum machine learning algorithms.
- Explore advanced quantum machine learning concepts, such as quantum neural networks and quantum optimization.

Unit I
Why Quantum Computing, History of Quantum Physics, Qubits, superposition, Probabilistic interpretation, Bloch sphere, Interference, Two Qubit states, Entanglement, Qubits versus Bits

Unit II
Forms of quantum computing, Quantum Computing: Abstraction Levels, Quantum Circuit, Quantum Operators and Gates, Identity operators, Unitary operator, Pauli Group of Matrices and Gates, Phase Gates, Cartesian Rotation Gates, Hadamard Gate, CNOT Gate, SWAP Gate, Density Operator Single-qubit operators, Multi-qubit operators.

Unit III
Data Representations, Basis encoding, Amplitude encoding, Dynamic encoding, Tensor Product Encoding, Hamiltonian Encoding, Quantum Algorithms Deutsch-Jozsa, Grover's Search, and Shor's Algorithm, Quantum PCA. Linear Models, Quantum k-means Clustering.

Unit IV
HHL Alogrithm , QUBO, Variational Quantum Ciruits, Supervised Learning, Quantum, Variational Quantum Eigensolver (VQE) and Quantum Approximate Optimization Algorithm (QAOA), Support Vector Machines, Quantum Computing with D Wave, Unsupervised Learning and Optimization.

Unit V
Quantum Deep Neural Networks, TSP (qbsolve), QNN with TensorFlow Quantum, Quantum CNN, Ensembles and QBoost, Quantum Image Processing, Ising Model

Textbooks
1. Ganguly, Santanu. Quantum Machine Learning: An Applied Approach. Apress, 2021.
2. Schuld, Maria, and Francesco Petruccione. Machine learning with quantum computers. Berlin: Springer, 2021.
3. Simeone, Osvaldo. "An introduction to quantum machine learning for engineers." Foundations and Trends® in Signal Processing 16.1-2 (2022): 1-223.

CSE612E	**Natural Computing Algorithms**	Credits: 04 L T P 3 0 2

Course Outcomes
- Understand the foundational principles of nature computing, including its philosophy.
- Understand evolutionary computing, exploring genetic algorithms, evolutionary programming, and genetic programming,
- Explore the concept of swarm intelligence, focusing on ant colony optimization, swarm robotics.
- Understand immune system's role in computing, including pattern recognition, immune network theory, and development of immune algorithms
- Students will be introduced to DNA Computing foundational experiments, and the potential shift from classical to DNA computing.

Unit I
From Nature to Nature Computing, Philosophy, Three Branches: A Brief Overview, Individuals, Entities and agents Parallelism and Distributivity Interactivity Adaptation Feedback-Self-Organization-Complexity, Emergence, Bottom-up Vs Top-Down- Determination, Chaos and Fractals.

Unit II
Evolutionary Computing, Hill Climbing and Simulated Annealing, Darwin's Dangerous Idea, Genetics Principles, Standard Evolutionary Algorithm –Genetic Algorithms, Reproduction-Crossover, Mutation, Evolutionary Programming, Genetic Programming

Unit III
Introduction Ant Colonies, Ant Foraging Behavior, Ant Colony Optimization, SACO and scope of ACO algorithms, Ant Colony Algorithm (ACA), Swarm Robotics, Foraging for food, Social Adaptation of Knowledge, Particle Swarm Optimization (PSO)

Unit IV
Introduction- Immune System, Physiology and main components, Pattern Recognition and Binding, Immune Network Theory- Danger Theory, Evaluation Interaction Immune Algorithms, Introduction – Genetic algorithms, Bone Marrow Models, Forest's Algorithm.

Unit V
DNA Computing: Motivation, DNA Molecule, Adleman's experiment, Test tube programming language, Universal DNA Computers, PAM Model, Splicing Systems.

Textbooks
1. Leandro Nunes de Castro, " Fundamentals of Natural Computing, Basic Concepts, Algorithms and Applications", Chapman & Hall/ CRC, Taylor and Francis Group, 2007
2. Brabazon, Anthony, Michael O'Neill, and Seán McGarraghy. Natural computing algorithms. Vol. 554. Berlin: Springer, 2015.
3. Floreano D. and Mattiussi C., "Bio-Inspired Artificial Intelligence: Theories, Methods, and Technologies", MIT Press, Cambridge, MA, 2008.
4. Albert Y.Zomaya, "Handbook of Nature-Inspired and Innovative Computing", Springer, 2006.

CSE577E	**Optimization Techniques for Machine Learning**	Credits: 03 L T P 3 0 0

Course Outcomes
- Understanding of linear algebra, differentiation, and multivariate calculus fundamentals crucial for optimization.
- Identify and solve convex optimization problems, leveraging concepts of convexity, duality, and optimality conditions.
- Proficiency in addressing constrained optimization challenges using Lagrangian, KKT conditions, and various algorithms for constrained optimization.
- Capability to implement and analyze gradient descent variants, Newton's method, and other advanced optimization algorithms for machine learning.
- Application of optimization techniques to solve real-world machine learning problems, enhancing computational efficiency and solution accuracy.

Unit I
System of Linear Equations; Vector space and sub-spaces (definition, examples, and concepts of basis); Linear mappings; Matrices; Eigenvalues and Eigenvectors Norms; Inner Product; Orthogonally; Spectral Decomposition; Singular value Decomposition, Differentiation of univariate functions, partial derivatives and gradients, Linearization and Multivariate Taylor Series.

Unit II
Convex sets examples and properties, convex functions strict and strong convexity, examples, and convexity preserving operations, Strong and weak duality, Maxima, minima, stationary point, saddle point, local and global maximum/minimum, First order and second order conditions for optimality, Linear, quadratic and convex optimization problems.

Unit III
Constrained optimization problem, feasible set, Lagrangian, KKT conditions, Linear and quadratic optimization, Duality for convex optimization theorem of alternatives, Farka's lemma, Algorithms for constrained optimization: Projected gradient descent, dual ascent, alternating direction method of multipliers.

Unit IV
Gradient descent normalized and normalized versions, Step size selection and convergence, Conservative theoretical guarantees and line search, Formal principles of gradient descent, Steepest descent norm generalization, Stochastic gradient descent (SGD), Mini-batch gradient descent, Momentum-based methods, Adaptive learning rate algorithms (e.g., Adam, RMSprop)

Unit V
Newton's method basics normalized and normalized versions, Newton's method, step size, and backtracking line search, scaling issues with Newton's method, Newton and secant method as zero-finding algorithms, Conjugate gradient and Quasi-Newton Methods.

Textbooks
1. Beck, First-Order Methods in Optimization, MOS-SIAM Series on Optimization, 2017.
2. S. Bubeck, Convex Optimization: Algorithms and Complexity, Foundations and Trends in Optimization, 2015.
3. F. Bach, "Learning with Submodular Functions: A Convex Optimization Perspective", Foundations and Trends in Machine Learning, Now Publishers Inc.

CSE611E	**Data Visualization**	Credits: 04 L T P 3 0 2

Course Outcomes
- Understand visualization principles and their impact on data interpretation.
- Master preprocessing and visualization techniques for diverse data types.
- Gain proficiency in Python-based and commercial visualization tools.
- Design interactive dashboards and web-based visualizations.
- Apply visualization techniques to real-world problems.

Unit I: Fundamentals of Data Visualization
Introduction to Data Visualization: Definition, Importance, Applications; Human Perception: Visual Encoding (Color, Shape, Size, Position), Cognitive Load; Exploratory Data Analysis (EDA): Univariate, Bivariate, Multivariate Analysis; Chart Types: Line, Scatter, Histogram, Bar (Stacked), Pie, Box, Hex Bin, Violin, Heatmaps, Gantt Charts, Word Clouds; Data Types: Categorical, Ordinal, Quantitative; Design Principles: Clarity, Accuracy, Avoiding Misleading Visuals.

Unit II: Visualization with Python (Pandas and Matplotlib)
Pandas: Setting up Environment, Data Loading (CSV, JSON), Basic Plots (Line, Bar, Histogram, Box, Area, Scatter, Pie, Subplots);
Matplotlib: Environment Setup, Line, Scatter, Histogram, Bar, Pie, Box, Doughnut, Word Clouds; Customization: Controlling Ticks (xlim, ylim, xticks, yticks), Labeling.
Nested Pie Plots; Polar Plots: Introduction, Bar, Line, Scatter on Polar Axis.

Unit III: Advanced Visualization with Seaborn
Seaborn: Environment Setup, Statistical Visualization; Customizations: Background Color. Grids. Despine, Scaling Plots/Fonts, rc Parameters; Univariate Distributions: Histogram, KDE Plot; Bivariate Distributions: Hex Plot, KDE Plot, Boxen Plot, Ridge Plot; Multivariate Visualizations: Pair Plots.
Facet Grids, Swarm Plots, Violin Plots.

Unit IV: Power BI for Visualization
Power BI: Components (Desktop, Service, Mobile Apps), Ecosystem, Workflow; Data Import: Excel. Web, SQL Server; Power Query: Data Cleaning, Transformation, Modeling Relationships: Visualization Types: Charts, Graphs, Maps, Custom Visuals; Advanced Features: DAX Basics, Calculated Fields, Filters.

Unit V: Interactive and Web-based Visualizations
Plotly: Features, Line, Area, Bar, Scatter, Pie, Bubble, Box, Histogram, Heatmaps, Gantt Charts, Word Clouds; Dash: Components (HTML, Core, Markdown), Callbacks (Single, Multiple Input/Output); Web Technologies: HTML, CSS, JavaScript Basics for Visualization; Advanced Topics: Geospatial Visualization (Maps, Choropleths), Big Data Visualization (Introduction to Apache Superset).

List of Practicals

1. Load the UCI Iris dataset, analyze features, and create bar and scatter plots. Tools: Python (Pandas, Matplotlib), Dataset: UCI Iris Dataset

2. Clean the Kaggle Titanic dataset (handle missing values, normalize data) and create a histogram. Tools: Python (Pandas, Matplotlib), Dataset: Kaggle Titanic Dataset

3. Create a line plot and pie chart with custom ticks, labels, and colors. Tools: Python (Matplotlib. Pandas), Dataset: Use any dataset

4. Generate pair plots and violin plots for a multivariate dataset. Tools: Python (Seaborn, Pandas), Dataset: Kaggle Boston Housing Dataset

5. Create a KDE plot and hex plot for a dataset with numerical features. Tools: Python (Seaborn, Pandas), Dataset: UCI Auto MPG Dataset

6. Import a retail dataset, transform it with Power Query, and create a dashboard with charts and filters. Tools: Power BI Desktop, Dataset: Kaggle Superstore Dataset

7. Create a visualization with a custom visual and a calculated field using DAX. Tools: Power BI Desktop, Dataset: Kaggle Sales Dataset

8. Create an interactive scatter plot with hover tooltips and filters using Plotly. Tools: Python (Plotly, Pandas), Dataset: Kaggle Gapminder Dataset

9. Build a dashboard with Plotly Dash, including a bar chart and callback-driven filters. Tools: Python (Plotly Dash, Pandas), Dataset: Kaggle COVID-19 Dataset

10. Visualize a dataset on a map using choropleths or point markers. Tools: Python (Plotly, Folium), Dataset: Kaggle US Crime Data

Textbooks
1. Tufte ER, Graves-Morris PR. The visual display of quantitative information. Cheshire, CT: Graphics press.
2. Knaflic CN. Storytelling with data: A data visualization guide for business professionals. John Wiley & Sons; 2015.

References
1. Mckinney W. Python for Data Analysis. O'Reilly Media; 2017.
2. VanderPlas J. Python data science handbook: Essential tools for working with data. O'Reilly Media, Inc.; 2016.
3. Deckler G. Learn Power BI: A beginner's guide to developing interactive business intelligence solutions using Microsoft Power BI. Packt Publishing Ltd; 2019.

Online Resources
1. https://www.datacamp.com/courses/introduction-to-data-visualization-with-python
2. https://www.kaggle.com/learn/data-visualization
3. https://learn.microsoft.com/en-us/power-bi/fundamentals/
4. https://www.freecodecamp.org/news/how-to-create-interactive-dashboards-in-python/

CSE625E	**Statistical Methods in Decision Making**	Credits: 03 L T P 3 0 0

Course Outcomes
- Understanding Statistics, its importance, terminologies, data sources, and the stages of conducting a statistical survey.
- Gain skills in data classification, tabulation, and presentation, along with calculating and interpreting measures of central tendency and dispersion.
- Develop a solid understanding of probability theory, including the calculation of probability, understanding of random variables, and probability distributions applicable in business contexts.
- Learn about the binomial and Poisson distributions, central limit theorem, and their significance.
- Students will be introduced to statistical inference, including estimation, hypothesis testing

Unit I
Basic Terminologies, Scope and Importance of Statistics. Sources of Data, Introduction to Methods of Primary and Secondary Data Collection. Statistical Survey: Definition of a Statistical Survey, Stages in a Statistical Survey: Planning and Execution, Sampling and Non-Sampling Errors

Unit II
Types of Data, Data Tabulation, Grouped Data and Ungrouped Data, Frequency Distribution, Histogram, Cumulative Frequency Distribution. Measures of Central Tendency: Mean, Median, Mode, Trimmed Mean; Measures of Dispersion: Range, Variance, Standard Deviation, Quantiles, Absolute Mean Deviation, and Coefficient of Dispersion. Symmetric, Positively and Negatively Skewed Distributions, Skewness and Extreme Values and Outliers, Boxplot.

Unit III
Definition of Probability: Introduction to Unconditional Probability, Simple Problems on Probability, Addition Rule of Probability, Conditional Probability, Multiplication Rule of Probability, Concept of Independent Events, Bayes Theorem. Definition of Random Variable, Introduction to Probability Distribution – Discrete and Continuous, Definition of Probability Mass Function and Cumulative Probability Mass Function.

Unit IV
PMF of Binomial and Poisson distributions, Expectation and Variance of Binomial and Poisson Distributions, Central Limit Theorem, Applications of Central Limit Theorem, Sampling Distribution of Sample Proportions

Unit V
Estimation Problem, Point Estimate and Interval Estimate, Margin of Error Introduction to Hypothesis Testing Problem, Null and Alternative Hypotheses, Type I and Type II Errors, Rejection and Acceptance Region, P-value
Z-test, Test of Normal Means: One-sample, Paired-sample, Two-sample. Introduction to t-distribution, Chi Square test, ANOVA, Pearson Correlation, Scatter Plot, Simple Regression, Introduction to Multiple Regression

Textbooks
1. Statistics for Business and Economics" by Paul Newbold, William L. Carlson, and Betty Thorne.
2. Applied Statistics in Business and Economics" by David Doane and Lori Seward.
3. Business Statistics: A First Course" by David M. Levine, Kathryn A. Szabat, and David F. Stephan.

CSE626E	**AI in Cyber Security**	Credits: 03 L T P 3 0 0

Course Outcomes
- Mastery of AI Fundamentals in Cybersecurity Context: Gain a solid understanding of artificial intelligence's core principles, including machine learning techniques such as classification, regression, and clustering, specifically applied within the realm of cybersecurity.
- Skill in Developing AI Models for Threat Detection: Develop the ability to construct and train AI models using algorithms like Perceptron's, Support Vector Machines (SVMs), Logistic Regression, Decision Trees, and Naive Bayes for the detection of various cybersecurity threats, including spam, phishing, and image-based attacks.
- Cybersecurity Data Analysis Expertise: Master advanced AI techniques like NLP and image processing to analyze and neutralize cybersecurity threats efficiently.
- Cloud AI Fraud Prevention Capability: Harness cloud AI, including machine learning, bagging, and boosting, for effective fraud detection. Gain hands-on experience with IBM Watson and Jupyter Notebooks for model development and evaluation.

Unit I
Applying AI in cyber security, The evolution from expert systems to data mining and AI, The different forms of automated learning, The characteristics of algorithm training and optimization, Beginning with AI via Jupyter Notebooks, introducing AI in the context of cyber security.

Unit II
Classification, Regression, Dimensionality reduction, Clustering Speech recognition, Video anomaly detection, Natural language processing (NLP), Large-scale image processing, and Social media analysis.

Unit III
How to detect spam with Perceptrons, Image spam detection with support vector machines (SVMs), Phishing detection with logistic regression and decision trees, Spam detection with Naive Bayes, and Spam detection adopting NLP.

Unit IV
 Protecting Sensitive Information and Assets
Authentication abuse prevention, Account reputation scoring, User authentication with keystroke recognition, Biometric authentication with facial recognition.

Unit V
How to leverage machine learning (ML) algorithms for fraud detection, how bagging and boosting techniques can improve an algorithm's effectiveness, how to analyze data with IBM Watson and Jupyter Notebook, how to resort to statistical metrics for results evaluation

Textbooks
1. Dr. Nilakshi Jain (2019). Artificial Intelligence, As per AICTE: Making a System Intelligent, Wiley Publication.
2. Alessandro Parisi .(2019). Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber-attacks and detecting threats and network anomalies, Packt Publication

CSE627E	**Generative Adversarial Networks**	Credits: 03 L T P 3 0 0

Course Outcomes
- Understand fundamental knowledge of generative adversarial network architectures.
- Understand deep learning principles underlying GANs, including neural network architectures and optimization techniques,
- Design and implementation of various advanced GAN models, such as cGANs, DCGANs, and WGANs
- Application of GANs to a range of domain-specific tasks.
- Explore the cutting-edge research and emerging trends in GANs, including their integration with other deep learning paradigms.

Unit I
Introduction to Generative Models, Genesis of GANs: History and Evolution, GAN Architecture: Generator and Discriminator Basics, Loss Functions and Evaluation Metrics for GANs, GAN Training Challenges and Solutions, Applications of GANs in Different Fields, Variants of GANs: An Overview, Ethical Considerations and Potential Misuses of GANs

Unit II
Introduction to Deep Learning and Neural Networks. Activation Functions, Batch Normalization, and Regularization Techniques, Deep Dive into Convolutional Neural Networks (CNNs), Optimizers and Learning Rate Strategies, Introduction to TensorFlow and PyTorch for GAN Development

Unit III
Conditional GANs (cGANs) and Their Applications, Deep Convolutional GANs (DCGANs): Architecture and Implementation, Wasserstein GANs (WGANs) and Gradient Penalty (WGAN-GP), Understanding and Implementing Cycle GANs for Image-to-Image Translation.

Unit IV
GANs in Art and Creativity: From Style Transfer to Novel Creations, Application of GANs in Healthcare: Data Augmentation and Anonymization, GANs for Enhancing Computer Vision Tasks, Using GANs for Natural Language Processing.

Unit V
Challenges in GAN Research, Unsupervised and Semi-supervised Learning with GANs GANs and Reinforcement Learning, GANs for Audio, Music, and Text, Integrating GANs with Other Deep Learning Paradigms.

Textbooks
1. Langr, Jakub, and Vladimir Bok. "GANs in action: deep learning with generative adversarial networks." (2019).
2. Kalin, Josh. Generative Adversarial Networks Cookbook: Over 100 Recipes to Build Generative Models Using Python, TensorFlow, and Keras. Packt Publishing Ltd, 2018.
3. Ganguly, Kuntal. Learning generative adversarial networks: next-generation deep learning simplified. Packt Publishing, 2017.
4. Kaddoura, Sanaa. A Primer on Generative Adversarial Networks. Springer Nature, 2023.

CSE609E	**Machine Learning for IoT**	Credits: 04 L T P 3 0 2

Course Outcomes
- Identify and understand the machine learning elements and techniques
- Implement data preprocessing methods for IoT using python
- Compare Machine Learning and Deep Learning
- Identify and understand Machine Learning accelerators for IoT Devices
- Design & implement deep learning model for sensor data
- Compare advanced machine learning techniques
- Design various IoT applications using ML and DL techniques.

Unit I
Introduction to Machine Learning: Introduction to ML, Introduction to Statistical Learning Methods, Classic and adaptive machines, Machine-Learning Problem, Machine-Learning Techniques and Paradigms, Machine Intelligence, Elements of Machine Learning, Introduction to Advanced ML Deep Learning, Reinforcement Learning.

Unit II
IOT Data Pre-processing: Data Preparation for Predictive Maintenance Modeling, Cleaning and Standardizing IoT Data, Applying Advanced Data Exploration Techniques Feature Engineering: Exploring Feature Engineering, Applying Feature Selection Techniques, Feature set selection using ML, Machine learning for Internet of Things data analysis.

Unit III
Machine learning (ML) methods for IoT Applications: Decision Trees (DTs), Support Vector Machines (SVMs), Bayesian theorem-based algorithms, kNearest neighbour (KNN), Random forest (RF), Association Rule (AR) algorithms, Ensemble learning (EL), k-Means clustering, Principal component analysis (PCA).

Unit IV
Compact fast Machine Learning Accelerators for IOT devices: Edge Computing on IOT Devices, IOT Based Smart Buildings, Distributed Machine Learning, Machine Learning Accelerator, Machine Learning Model Optimization, Least-Squares-Solver for Shallow Neural Network: Introduction, Algorithm Optimization, Hardware Implementation.

Unit V
Applications of ML and IOT: Case Studies: IOT for Agriculture, Remote Patient Monitoring, Smart City, Smart Transportation, IOT Security using ML.

List of Practicals

1. IoT Data Cleaning & Outlier Detection: Preprocess noisy sensor data for ML.

2. Feature Extraction from Vibration Sensors: Extract time-frequency features for predictive maintenance.

3. Predictive Maintenance with Decision Trees: Train an interpretable model for equipment failure.

4. Anomaly Detection using k-Means: Cluster smart meter data to detect fraud.

5. Edge Deployment of SVM on Raspberry Pi: Classify sounds in real-time on edge.

6. Federated Learning Simulation: Train a model without centralized data.

7.   Traffic Prediction with XGBoost: Forecast traffic flow using ensemble learning.

8. Real-Time IoT Dashboard: Visualize live sensor data with ML insights.

9. Adversarial Attack on Face Recognition: Fool an IoT camera model with adversarial noise.

Textbooks
1. Ethem ALPAYDIN, "Introduction to Machine Learning", The MIT Press, October 2004, ISBN 0-262-01211-1

2. Hantao Huang, Hao Yu, "Compact and Fast Machine Learning Accelerator for IoT Devices,"Edition: 1st ed. Publisher: Springer Singapore Year: 2019ISBN: 978-981-13-3323- 1

References

1. Trevor Hastie Robert Tibshirani Jerome Friedman, "The Elements of Statistical Learning: Data Mining, Inference, and Prediction", Second Edition, Springer Series in Statistics, Feb 2009
2. Tom M. Mitchell, "Machine Learning", McGraw-Hill Science/Engineering/Math; (March 1, 1997) ISBN: 0070428077
3. Neeraj Kumar, Aaisha Makkar, "MACHINE LEARNING IN COGNITIVE IOT", https://www.routledge.com/Machine-Learning-in-Cognitive-IoT/KumarMakkar/p/book/9780367359164 ISBN 9780367359164 Published June 1, 2020 by CRC Press
4. Puneet Mathur, "IoT Machine Learning Applications in Telecom, Energy, and Agriculture, With Raspberry Pi and Arduino Using Python", ISBN 978-1-4842-5549-0
5. Nicolas Modrzyk, "Real-Time IoT Imaging with Deep Neural Networks Using Java on the Raspberry Pi 4", Apress Publication, Year: 2020, ISBN: 9781484257210, 978148425722

Online Resources

1. Predictive Analytics for IOT, by Microsoft on edx
2. Link: https://www.edx.org/course/predictive-analytics-for-iotsolutions?source=aw&awc=6798_1594277292_cca42f86ac9afe29904595a53aad9e1c
3. INTERNET of Things and Machine Learning Training
4. Link: https://shop.boltiot.com/products/internet-of-things-and-machine-learning-training

VERTICAL IV: GENERAL

CSE562E	**Advanced Database Systems**	Credits: 04 L T P 3 0 2

Course Outcomes
- To understand the basic concepts and terminology related to DBMS and Relational Database Design
- To implement complex queries including full outer joins, self-join, sub
- queries, and set theoretic queries.
- To understand file organization, Query Optimization, Transaction management, and database administration techniques
- To the design and implement Distributed Databases.
- To understand advanced DBMS techniques to construct tables and write effective queries, forms, and reports.

Unit I
Formal review of relational database and FDs Implication, Closure, its correctness

Unit II
3NF and BCNF, Decomposition and synthesis approaches, Review of SQL99, Basics of query processing, external sorting, file scans
.
Unit III
Processing of joins, materialized vs. pipelined processing, query transformation rules, DB transactions, ACID properties, interleaved executions, schedules, serialisability.

Unit IV
Correctness of interleaved execution, Locking and management of locks, 2PL, deadlocks, multiple level granularity, CC on B+ trees, Optimistic CC

Unit V
T/O based techniques, Multiversion approaches, Comparison of CC methods, dynamic databases, Failure classification, recovery algorithm, XML and relational databases

Textbooks
1. R. Ramakrishnan, J. Gehrke, Database Management Systems, McGraw Hill, 2004
2. Silberschatz, H. Korth, S. Sudarshan, Database system concepts, 5/e, McGraw Hill, 2008.

References
1. Elmasri, Ramez, and Shamkant B. Navathe. "Fundamentals of Database Systems 7th ed." (2016).

CSE563E	**Semantic Web Technologies**	Credits: 04 L T P 3 0 2

Course Outcomes
- Demonstrate the semantic web technologies like RDF Ontology and others.
- Learn the various semantic web applications.
- Identify the architectures and challenges in building social networks.
- Analyze the performance of social networks using electronic sources.

Unit I
Traditional web to semantic web – WWW and its usage- meta data and its creation, addition in the web page; meta data tools – search engines for semantic web –search engine for web page mark up problem and query building problem. Web Intelligence Thinking and Intelligent Web Applications, The Next Generation Web, Semantic Road Map, Logic on the semantic Web.

Unit II
Knowledge Representation for the Semantic Web Ontologies and their role in the semantic web, Ontologies Languages for the Semantic Web – Resource Description Framework(RDF) / RDF Schema, Ontology Web Language(OWL), UML, XML/XML Schema.

Unit III
The basics idea of Web ontology language– OWL to define classes- OWL to define properties-set operators-Three faces of OWL-Ontology Matching and Distributed Information- Validating OWL ontology, Ontology Libraries and Ontology Mapping, Logic, Rule and Inference Engines.

Unit IV
Web services – web services standards – web services
to semantic web services- UDDI and its usage- Concept of OWL-S and its building blocks – mapping OWL-S to UDDI-WSDL-S overview and its usage.

Unit V
Semantic Web Applications, REAL WORLD EXAMPLES AND APPLICATIONS OF SEMANTIC WEB (9hours) Swoogle architecture, usage and examples of using Swoogle; FOAF – Explanation, vocabulary –creating FOAF documents – overview of semantic markup – semantic web search engines.

Textbooks
1. Liyang Yu, "Introduction to the Semantic Web and Semantic web services" Chapman & Hall/CRC, Taylor & Francis group, 2007.

References
1. Johan Hjelm, "Creating the Semantic Web with RDF ", Wiley, 2001.
2. Grigoris Antoniou and Frank van Harmelen, "A Semantic Web Primer", MIT Press, 2004.
3. Karin K. Breitman K., Marco Antonio Casanova, Walt Truszkowski, "Semantic web concepts, Technologies and applications" Walt Truszkowski 2007.
4. Semantic Web Technologies, Trends and Research in Ontology Based Systems.
5. Semantic Web and Semantic Web Services -Liyang Lu Chapman and Hall/CRC Publishers, (Taylor & Francis Group).
6. Programming the Semantic Web, T.Segaran, C.Evans, J.Taylor, O'Reilly.

CSE578E	**Graph theory**	Credits: 03 L T P 3 0 0

Course Outcomes
- Understand the basics of graph theory and their various properties.
- Model problems using graphs and to solve these problems algorithmically.
- Evaluate or synthesize any real world applications using graph theory.

Unit I
Introduction to Graphs and Graph data structure, Graph Terminology: vertices, edges, weight, degree, path, walk, trial, cycle, connectedness, planarity, bipartiteness, adjacency and incidence. Types of Graphs, Representation of graphs and graph isomorphism: Adjacency matrix, Incidence matrix, circuit matrix, adjacency list.

Unit II
BFS and DFS in a graph. Shortest Path Algorithms & Traversability: Shortest Path, distances, eccentricity, Dijkstra's algorithm for the single source shortest paths, Floyd's algorithm for all pair shortest paths. Eulerian trails and Hamiltonian paths.

Unit III
Trees & Applications: Trees, Properties, rooted trees, Rooted & Binary Trees, Prefix codes, Binary codes, Huffman's Algorithm, Spanning trees, Kruskal's and Prim's algorithms for the optimal spanning tree.

Unit IV
Networks: Flow in Graphs: Max-Flow-Min-cut theorem, Algorithm for Max-Flow, Manger's Theorems, Feasible Flows.

Unit V
Planarity and Colouring: Independent set, Planar graphs, Directed graphs, Kuratowski graphs, Different representations of planar graphs. Edge colouring, vertex colouring, critical graphs, chromatic polynomials.

Textbooks
1. Narsingh Deo, Graph theory with Applications to Engineering & CS, PHI
2. Alan Gibbons, Algorithmic Graph theory, Cambridge University Press
3. Jeffrey J. McConnell, Analysis of algorithms, Narosa, 2004
4. Humdy A Taha, Operation Research, TMH, 2003.
5. Harary F, Graph Theory, Narosa, 1993.

CSE580E	**Modern Operating Systems**	Credits: 03 L T P 3 0 0

Course Outcomes
- Explore the history and evolution of operating systems, delving into computer hardware and the diverse operating system concepts.
- Understand processes, threads, and intercommunication within operating systems, including scheduling and classical IPC problems.
- Gain insights into memory management, virtual memory, and segmentation, along with file system implementation and optimization.
- Learn principles of input/output hardware and software, covering input/output software layers, devices, and user interfaces.
- Explore advanced topics such as virtualization, cloud computing, security considerations, and operating system design principles, including case studies of Unix, Windows 8, and Android.

Unit I
Introduction: History, Computer hardware, Operating system Zoo, Operating system concepts, System calls, operating system structure. Processes and threads, Intercommunication communication, Scheduling, Classical IPC problems.

Unit II
Memory management, Memory abstraction, Virtual memory, page replacement algorithms, design issues for paging systems, implementation issues, Segmentation, File system, Directories. Directories. File system implementation and optimization with examples.

Unit III
Input output Principles of input/output hardware and software, Input/output software layers, disks, clocks, user interfaces: keyboards, mouse, monitor, thin client, power management. Deadlocks. Deadlocks. Deadlock avoidance prevention and other issues. Deadlock avoidance prevention and other issues

Unit IV
Virtualization and the cloud, Memory virtualization, Input/output virtualization. Memory virtualization, Input output virtualization. Virtual machines on multicore CPUs. Licensing issues, Clouds as a service, Virtual machine migration, check pointing, VMWARE

Unit V
Multiple processor systems, Multi computers, Distributed systems, security, security environment. Operating system security, Controlling access to resources. Formal models and secure systems. Basics of cryptography, Authentication, exploiting software, insider attacks, malware defenses, Case study Unix, Windows 8 and Android, Operating system design

Books
1. "Modern Operating Systems" by Andrew S. Tanenbaum and Herbert Bos, Fourth edition

CSE564E	**Back End Development Technologies**	Credits: 04 L T P 3 0 2

Course Outcomes
- Understand the basics of back end development.
- Understanding and implementing databases.
- Implementation in server-side frameworks.
- Understanding Deployment and scalability.

Unit I
Overview of Back End Development: Roles and Responsibilities, Client-Server Architecture and the Role of the Back End, Introduction to Server-Side Programming Languages: Python, JavaScript (Node.js), Ruby, Java, etc. Setting up

Unit II
Introduction to Relational and Non-Relational Databases, Database Design and Modelling: Entity-Relationship Diagrams (ERD), SQL Fundamentals: Querying, Joins, Indexes, and Transactions, NoSQL Databases: Document, Key-Value, Columnar, and Graph Databases, Hands-on Lab: Implementing Database Solutions using MongoDB

Unit III
Introduction to Server-Side Frameworks: Express.js, Routing and Middleware Concepts in Web Frameworks, User Authentication and Authorization: Sessions, Cookies, Handling HTTP Requests and Responses: RESTful APIs, Building RESTful APIs with Express.js.

Unit IV
Common Web Security Threats: Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), SQL Injection, etc.
Security Best Practices: Input Validation, Output Encoding, Parameterized Queries
Authentication and Authorization Mechanisms: OAuth, Role-Based Access Control (RBAC)

Unit V
Deployment Strategies: Monolithic vs. Microservices Architecture, Containerization and Orchestration with Docker and Kubernetes, Cloud Computing Platform: AWS, Monitoring and Scaling Back-End Services for High Availability and Performance

Textbooks
Node.js Design Patterns" by Mario Casciaro
RESTful Web APIs: Services for a Changing World" by Leonard Richardson and Mike Amundsen

References
"Learning Web Design: A Beginner's Guide to HTML, CSS, JavaScript, and Web Graphics" by Jennifer Niederst Robbins
Online Documentation and Tutorials from Official Documentation of Express.js, Django, Flask, Node.js, etc.

CSE579E	**Human-Computer Interaction**	Credits: 03 L T P 3 0 0

Course Outcomes
- Imagine alternatives to traditional "keyboard and mouse" computing.
- Appreciate the importance of a design and evaluation methodology that begins with and maintains a focus on the user.
- Develop familiarity with a variety of non-traditional user interface paradigms such as virtual and augmented reality, mobile and wearable computing, and ubiquitous computing.
- Develop ability to design certain tools for blind and specially-abled people.

Unit I
Human interaction with computers, importance of user interface, definition, importance of a good design, the graphical user interface, popularity of graphics, the concept of direct manipulation, graphical system, characteristics, interface popularity, principles of user interface.

Unit II
Understanding business junctions, screen designing, design goals, screen planning and purpose, organizing screen elements, ordering of screen data and content, screen navigation and flow, visually pleasing composition.

Unit III
Amount of information, presentation of information simply and meaningfully, information retrieval on web, statistical graphics, the software life cycle, usability engineering, iterative design and prototyping, prototyping in practice, design rationale, design rules, principles to support usability, standards, Golden rules and heuristics

Unit IV
HCI patterns, evaluation techniques, goals of evaluation, evaluation through expert analysis, evaluation through user participation, multi-modal interaction, cognitive models, goal and task hierarchies, linguistic models, the challenge of display-based systems, physical and device models, cognitive architectures.

Unit V
Ubiquitous computing and augmented realities, ubiquitous computing applications research, Ambient Wood – augmenting the physical, virtual and augmented reality, applications of augmented reality, information and data visualization, ethics and responsibility.

Textbooks
1. Alan Dix, Janet Fincay, Gre Goryd, Abowd, Russell Bealg: Human–Computer Interaction (Pearson Education)
2. Rogers, Sharps: Interaction Design Prece (Wiley Dreamtech)
3. Soren Lauesen: User Interface Design (Pearson Education)
4. D. R. Olsen: Human –Computer Interaction (Cengage Learning.)

CSE565E	**High Performance Computing Systems**	Credits: 04 L T P 3 0 2

Course Outcomes
- Describe and use the main design techniques for sequential and parallel algorithms.
- Understand the architecture of modern CPU's and how this architecture influences the way programs should be written.
- Understand the differences among parallel and sequential algorithms solving the same problem and recognize which one is better under different conditions.
- Understand parallel algorithm for different architectures
- Describe and use basic and advanced parallel algorithms

Unit I

Modern Processors: Stored Program Computer Architecture General purpose cache- based microprocessor, Moore's Law, Pipelining, SIMD- Memory Hierarchies Cache- mapping- prefetch- Multicore processors, Multithreaded processors, Vector Processors- Design Principles- Maximum performance estimates

Unit II

Parallel Computers: Taxonomy of parallel computing paradigms Shared memory computers, Cache coherence- UMA, ccNUMA Distributed-memory computers, Hierarchical systems, Switched and fat- tree networks, Mesh networks, Basics of parallelization -Why parallelize, Data Parallelism, Function Parallelism, Parallel Scalability-,Factors that limit parallel execution.

Unit III

Distributed memory parallel programming with MPI : message passing introduction to MPI – example messages and point-to-point communication collective communication – non blocking point-to-point communication.

Unit IV

Shared memory parallel programming with OpenMp : introduction to OpenMp parallel execution data scoping- OpenMp work sharing for loops- synchronization reductions loop scheduling – tasking

Unit V

Efficient MPI programming: MPI performance tools communication parameters- Synchronization, serialization, contention- Reducing communication overhead- optimal domain decomposition- Aggregating messages

Textbooks
1. Georg Hager, Gerhard Wellein, "Introduction to High Performance Computing for Scientists and Engineers", Chapman & Hall / CRC Computational Science series, 2011.

References
2. Charles Severance, Kevin Dowd, "High Performance Computing", O'Reilly Media, 2nd Edition, 1998.
3. Kai Hwang, Faye Alaye Briggs, "Computer Architecture and Parallel Processing", McGraw Hill, 1984.
4. Pacheco, Peter S., "Parallel Programming with MPI", Morgan Kaufmann Publishers, Inc., California, 1997.
5. Cook, Shane. CUDA programming: a developer's guide to parallel computing with GPUs. Newnes, 2012.

CSE581E	**Architecting Social Networks**	Credits: 03 L T P 3 0 0

Course Outcomes
- Illustrate the basic concepts of social network.
- Analyse the networks to find prominent actors and relate social network models.
- Develop social network applications using tools and techniques.
- Detect and analyse the commUnities in social networks.
- Design a system to assimilate information available on the web to model and build Social Network Application.

Unit I

Social Network Perspective, Fundamentals concepts in Network Analysis: Sociogram, Sociometry. Social Network Data: Types of Networks: One-Mode, Two-Mode, Affiliation, Ego-centered and Special Dyadic Networks, Network Data, Measurement and Collection, Notations for Social Network Data: Graphs, Directed, Singed, Valued graphs, Multigraph, Relations and Matrices.

Unit II

Prominence: Actor-Centrality, Prestige, Group-Centrality, Prestige, Non directional Relations-Degree, Closeness, Betweenness, Eigen Vector Centrality, Directional Relations-Centrality, Prestige.
Structural Balance: Signed Non directional, Signed Directional Relations, Checking for Balance, Index for Balance, Clusterability-Theorems, Clustering Coefficient and Transitivity.

Unit III

Social Group and Subgroup-Notation, Subgroups Based on Complete Mutuality: Clique, Reachability and Diameter: n-cliques, n-clans and n-clubs, Subgroups Based on Nodal Degree: k-plexes, k-cores, Measures of Subgroup Cohesion, Community detection using Subgroups and Betweenness.

Unit IV

Structural Equivalence: Definition, Social Roles and, Positional Analysis, Measuring Structural Equivalence, Representation of Network Positions, Block Models-Introduction, Network Positions and roles-Introduction
Dyads: Definitions, Dyad Census, Index, Simple Distributions, Triads: Random Models and Substantive Hypotheses, Testing Structural Hypotheses.

Unit V

Small world network- Watt Strogatz networks statistical models for social networks network evaluation model Preferential attachment power law Random Model: Erdos -Renyi model Barabasi Albert model Epidemic model Case study: Text and opinion Analysis

Textbooks
1. Wasserman Stanley, and Katherine Faust, Social Network Analysis: Methods and Applications, Structural Analysis in the Social Sciences. Cambridge University Press, 2012 Online Edition.
2. Albert-László Barabási, Network Science, Cambridge University Press, 1st edition, 2016.

References
1. John Scott, "Social Network Analysis", Sage Publications Ltd., Fourth Edition, 2017.
2. David Knoke & Song Yang, "Social Network Analysis", Sage Publishing, Third Edition, 2020.

CSE613E	**Front End Development Technologies**	Credits: 04 L T P 3 0 2

Course Outcomes
- Understand basic fundamentals of Front-end Technologies
- Demonstrate Proficiency in HTML, CSS, and JavaScript.
- Design Responsive and User-Friendly Web Interfaces.
- Utilize Front End Frameworks and Libraries.

Unit I
Protocols, Servers and their Functions, Internet Clients, Network Security, Internet Development, Design Functional Internet site & Business Concepts, Fundamentals/ Basic HTML 5, Text formatting on Web Pages, incorporate multimedia, Creating hyperlinks, tables and nested tables, Inserting web page, Setting & modifying field properties, Forms.

Unit II
Introduction, Designing with Style Sheets, Style Sheet Syntax, ID, Class Contextual Selectors, Cascading Order, Properties, Absolute and Relative Positioning, Layering Elements using Z-Index, Animating objects

Unit III
Introduction to JavaScript: Syntax, Data Types, and Variables.
Control Flow and Functions: Conditionals, Loops, and Error Handling.
DOM Manipulation: Selecting Elements, Events, and Event Handling.

Unit IV
Introduction to JavaScript Frameworks: Angular, and React, Understanding Component-Based Architecture.
Introduction to Angular JS, Angular Modules, Angular Components, Templates and Styles

Unit V
Work flow of React JS, Scope of React JS, Overview of Jsx, React Js Environment Setups, React component Properties, Setting Properties, Component Lifecycle, Updating Components, React.js component, Mounting Components, Event Handling, Expressions & Attributes, JSX Basics, Namespaced Components, Rendering HTML, Rendering React Components

Textbooks
1. "HTML and CSS: Design and Build Websites" by Jon Duckett
2. "Eloquent JavaScript: A Modern Introduction to Programming" by Marijn Haverbeke
3. References Books:
4. "Learning Web Design: A Beginner's Guide to HTML, CSS, JavaScript, and Web Graphics" by Jennifer Niederst Robbins
5. Documentation and Tutorials from Official Documentation of React, Angular, Vue.js

CSE614E	**Social Network Analysis and Mining**	Credits: 04 L T P 3 0 2

Course Outcomes
- understand the basic concepts of social networks
- understand the fundamental concepts in analyzing the large-scale data that are derived from social networks
- implement mining algorithms for social networks
- perform mining on large social networks and illustrate the results.

Unit I
Introduction to Social Network Mining, Graph Models and Node Metrics, Introduction to social network mining. Illustration of various social network mining tasks with real-world examples. Data characteristics unique to these settings and potential biases due to them. Social Networks as Graphs. Random graph models/ graph generators, degree distributions. Models of evolving networks. Node based metrics, ranking algorithms (Page rank), graph visualization and exploration software – practice.

Unit II
Social-Network Graph Analysis, Social network exploration/ processing: graph kernels, graph classification, clustering of social-network graphs, centrality measures, community detection and mining, degeneracy (outlier detection and centrality), partitioning of graphs. SNAP system for large networks analysis and manipulation.

Unit III
Social-Network Graph Analysis and Properties, Social network exploration/ processing and properties: Finding overlapping communities, similarity between graph nodes, counting triangles in graphs, neighborhood properties of graphs.

Unit IV
Information Diffusion in Social Networks, Strategic network formation: game theoretic models for network creation/ user behavior in social networks. Information diffusion in graphs: Cascading behavior, spreading, epidemics, heterogeneous social network mining, influence maximization, outbreak detection. Opinion analysis on social networks: Contagion, opinion formation, coordination and cooperation.

Unit V
Dynamic Social Networks, Applications and Research Trends, Dynamic social networks, Link prediction, Social learning on networks. Special issues in Information and Biological networks. Important applications of social network mining related to the above topics. Research trends

Textbooks
1. David Easley and Jon Kleinberg, Networks, crowds, and markets, Cambridge University Press, 2010.
2. Jure Leskovec, Anand Rajaraman and Jeffrey David Ullman, Mining of massive datasets, Cambridge University Press, 2014.

CSE631E	**Optimization Methods**	Credits: 03 L T P 3 0 0

Course Outcomes
- Model engineering minima/maxima problems as optimization problems.
- Learn efficient computational procedures to solve optimization problems.
- Enumerate fundamentals of Integer programming technique and apply different techniques to solve various optimization problems arising from engineering areas
- Be able to use MATLAB to implement optimization algorithms

Unit I
Mathematical preliminaries: Linear algebra and matrices, Vector space, eigen analysis, Elements of probability theory, Elementary multivariable calculus

Unit II
Linear Programming: Introduction to linear programming model, Simplex method, Duality, Karmarkar's method
Unconstrained optimization: One-dimensional search methods, Gradient-based methods, Conjugate direction and quasi-Newton methods

Unit III
Constrained Optimization: Lagrange theorem, FONC, SONC, and SOSC conditions.
Non-linear problems: Non-linear constrained optimization models, KKT conditions, Projection methods

Unit IV
Advanced Topics in Optimization: Piecewise linear approximation of a nonlinear function, Multi objective optimization – Weighted and constrained methods;

Unit V
Multi-level optimization, Direct and indirect search methods, Evolutionary algorithms for optimization and search, Applications in civil engineering

Textbooks
1. An introduction to Optimization by Edwin P K Chong, Stainslaw Zak
2. Nonlinear Programming by Dimitri Bertsekas

References
1. S.S. Rao,"Engineering Optimization: Theory and Practice", New Age International P)Ltd., New Delhi, 2000
2. G. Hadley,"Linear programming", Narosa Publishing House, New Delhi, 1990.
3. Latest Relevant Research Papers

CSE632E	**Algorithmic Game Theory**	Credits: 03 L T P 3 0 0

Course Outcomes
- Acquire insight into game-theoretic situations by experiencing them from the perspective of   an actual decision maker.
- Apply the tools learnt towards solution of various problems in computer science and Internet economics such as decentralized algorithms, sponsored search auctions on the web, procurement markets in electronic commerce, resource allocation mechanisms in computational grids, design of robust communication protocols, analysis of social networks.
- Pursue inter-disciplinary topics such as cyber-physical systems, intelligent transportation, service science, green supply chains, and human computation systems (such as crowdsourcing networks).

Unit I
Introduction to game theory, rationality, intelligence, common knowledge, References relations, expected utility, Von Neumann Morgenstern utilities

Unit II
Strategic form games, Normal form games (Pareto dominance), extensive form games, subgame perfect equilibrium, games with incomplete information, Bayesian games, zero sum and general sum games

Unit III
Nash equilibrium (pure strategy and mixed strategy equilibria), existence of Nash equilibrium, computation of Nash equilibrium, minimax theorem, matrix games, social choice functions and properties, incentive compatibility.

Unit IV
Revelation theorem, Gibbard-Satterthwaite theorem, Arrow's impossibility theorem, quasi-linear environment, VCG mechanism, Knapsack mechanism, dAGVA mechanisms, optimal auctions.

Unit V
Correlated equilibrium, two person bargaining problem, coalitional games (hedonic), Shapley value, stable matching, Gale-Shapley algorithm.

Textbooks
1. Noam Nisan, Tim Roughgarden, Eva Tardos, and Vijay Vazirani: Algorithmic Game Theory (Cambridge University Press, 2007)
2. Martin Osborne and Ariel Rubinstein: A Course in Game Theory (MIT Press, 1994)
3. Roger Myerson: Game Theory Analysis of Conflict (Harvard University Press, 1997)
4. Y. Narahari: Game Theory and Mechanism Design (IISc Press and the World Scientific, 2014)

CSE629E	**Application Development**	Credits: 03 L T P 3 0 0

Course Outcomes
- Describe requirement & Challenges in mobile application design & development
- Develop the design for mobile applications for specific requirements
- Implement the design using Andriod SDK, Objective C &iOS
- Deploy mobile applications in Andriod & iPhone market place for distribution.

Unit I
Fundamentals of Java for Android Application Development, Overview of Android, Developing Spectacular Android Applications, Your First Android Project, Using Activities, Fragments and Intents in Android, Creating the User Interface, Coding Your Application, Understanding Android Resources, Turning Your Application into an App Widget

Unit II
Designing the Tasks Application, Creating the Task Detail Page, Handling User Input, Getting Persistent with Data Storage, Updating Status Bar, Handling Pictures and Menus with Views, Emailing and Networking in Android, Working with Location Services and Maps, Working with Graphics and Animation, Audio, Video and Camera

Unit III
Reminding the User, working with Android PReferences, developing for Tablets, Supporting Older Versions of Android. Publishing Your App to the Google Play Store, Monetizing and Distributing Android Applications.
Bluetooth, NFC, and Wi-Fi, Telephony and SMS, Hardware Sensors

Unit IV
Introduction, Creating the RoadTrip User Interface, The Runtime, Managing Memory, and Using Properties, Working with the Source Editor, Adding Outlets and Actions to Your RoadTrip Code, Adding Animation and Sound to Your App.

Unit V
The Trip Model, Implementing the Master View Controller, Working with Split View Controllers and the Master View, Finishing the Basic App Structure, Working with Web Views, Displaying Events Using a Page View Controller, Finding Your Way, Geocoding, Finding a Location, Selecting a Destination.

Textbooks
1. Android App Development for Dummies, Michael Burton, Wiley
2. IOS App Development for Dummies, Jesse Feiler Wiley
3. Android Application Development Black Book, Pradeep Kothari, Dreamtech press.

References
1. Android Programming: The Big Nerd Ranch Guide; Bill Phillips and Brian Hardy; Publisher: Big Nerd Ranch Guides.
2. IOS Programming: The Big Nerd Ranch Guide,Christian Keur and Aaron Hillegass; Big Nerd Ranch Guides

CSE630E	**Advanced IoT Systems Integration and Industrial Applications**	Credits: 03 L T P 3 0 0

Course Outcomes
- Understanding role of edge computing in IoT.
- Understanding Role of cloud computing and security in IoT.
- Understanding the fusion of IoT with robotics and automation technologies
- Integration of machine learning with IoT

Unit I

Introduction to Edge Computing, Edge Devices and Gateway in IoT, Benefits and Challenges of Edge Computing, IoT Data Processing and Storage, Techniques for Analyzing IoT Data, Data-Driven Decision-Making in Industrial Applications.

Unit II

Overview of Cloud Service Models, Cloud Service Providers Evaluation Toolkit, Scalability and Resource Management in Cloud-Based IoT, Cloud-Based Data Integration, Cloud Cost Optimization Strategies

Unit III

Security Risks in IoT Systems, Privacy Concerns in IoT Applications, Security Measures for IoT Devices and Networks, Overview of IoT Regulations and Standards, Role of Compliance in IoT Security and Privacy.

Unit IV

Integration of IoT with Robotics and Automation Technologies, IoT-Enabled Robots and Cobots, Benefits and Challenges of IoT-Driven Automation, Strategies for IoT and Robotics Integration, Assessing the Impact of IoT-Driven Automation, Designing a Comprehensive IoT Solution with Robotics and Automation Technologies.

Unit V

Introduction to machine learning, Types- supervised, unsupervised, reinforcement, semi-supervised learning, features and feature selection techniques, bias and variance tradeoff, overfitting and under fitting, machine learning for mobile devices.

CASE STUDIES/INDUSTRIAL APPLICATIONS: IoT applications in home, infrastructures, buildings, security, Industries, Home appliances, other IoT electronic equipments, Industry 4.0 concepts

Textbooks
1. IoT Fundamentals: Networking Technologies, Protocols and Use Cases for Internet of Things, David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Rob Barton and Jerome Henry, Cisco Press, 2017
2. Internet of Things – A hands-on approach, Arshdeep Bahga, Vijay Madisetti, Universities Press, 2015

References
1. The Internet of Things – Key applications and Protocols, Olivier Hersent, DavidBoswarthick, Omar Elloumi and Wiley.
2. "From Machine-to-Machine to the Internet of Things – Introduction to a New Age of Intelligence",Jan Ho¨ ller, VlasiosTsiatsis, Catherine Mulligan, Stamatis, Karnouskos, Stefan Avesand. David Boyle and Elsevier.

CSE615E	**Social Network Security and Analysis**	Credits: 04 L T P 3 0 2

Course Outcomes
- Develop semantic web related simple applications.
- Address Privacy and Security issues in Social Networking.
- Explain the data extraction and mining of social networks
- Discuss the prediction of human behavior in social communities
- Describe the applications of social networks

Unit I
Introduction to Semantic Web, Limitations of current Web, Development of Semantic Web,
Emergence of the Social Web, Social Network analysis, Development of Social Network Analysis, Key concepts and measures in network analysis, Historical overview of privacy and security, Major paradigms, for understanding privacy and security

Unit II
The evolution of privacy and security concerns with networked technologies, Contextual influences on privacy attitudes and behaviours, Anonymity in a networked world

Unit III
Extracting evolution of Web Community from a Series of Web Archive, Detecting communities in social networks, Definition of community, Evaluating communities, Methods for community detection and mining, Applications of community mining algorithms, Tools for detecting communities social network infrastructures and communities, Big data and Privacy

Unit IV
Understanding and predicting human behavior for social communities, User data Management,
Inference and Distribution, Enabling new human experiences, Reality mining, Context, Awareness, Privacy in online social networks, Trust in online environment, What is Neo4j, Nodes, Relationships, Properties.

Unit V
Understand the access control requirements for Social Network, Enforcing Access Control Strategies, Authentication and Authorization, Roles-based Access Control, Host, storage and network access control options, Firewalls, Authentication, and Authorization in Social Network, Identity & Access Management, Single Sign-on, Identity Federation, Identity providers and service consumers, The role of Identity provisioning

Textbooks
1. Peter Mika, Social Networks and the Semantic Web, First Edition, Springer 2007.
2. BorkoFurht, Handbook of Social Network Technologies and Application, First Edition,
Springer, 2010

References
1. Easley D. Kleinberg J., Networks, Crowds, and Markets – Reasoning about a Highly Connected World‖, Cambridge University Press, 2010.
2. Jackson, Matthew O., Social and Economic Networks‖, Princeton University Press, 2008.

CSE616E	**Health Informatics**	Credits: 04 L T P 3 0 2

Course Outcomes
- Understand the fundamental concepts and historical development of Health Informatics
- Gain comprehensive knowledge of the standards and protocols and understand the significance of Clinical Decision Support Systems (CDSS)
- Understand the healthcare analytics pipeline, including the collection, analysis, and application of big data in healthcare.
- Understand the importance of privacy, security, and ethical considerations in Health Informatics, including compliance with HIPAA and the HITECH act.
- Identify and analyze emerging trends and technologies in Health Informatics

Unit I
Overview of Health Informatics, Definition and scope, Historical perspective,Key Players in Health Information Technology , Organizations involved with Health Informatics Healthcare Data and its Types Health Information Systems, Overview of Electronic Health Records (EHRs) and Electronic Medical Records (EMRs)

Unit II
Importance of health information exchange (HIE), Standards and protocols (HL7, FHIR)
Clinical Decision Support Systems (CDSS) and its Role in patient care, Examples and applications, Telehealth and Mobile Health (mHealth) Concepts and applications, Impact on healthcare delivery.

Unit III
Introduction to data analytics in healthcare, Analytics Pipeline Tools and techniques, Big Data in Healthcare, Challenges to Data Analytics, Research and Application of Analytics, Role of Informaticians in Analytics, Big data concepts, Use cases in healthcare, introduction to Machine Learning and AI in Healthcare, Basic concepts and applications.

Unit IV
HIPAA, Basic Security Principles, HIPAA meaningful use and HITECH act, Authentication and Identity Management, Data Security in Cloud and Client/ Server Solutions, Standards, Compliance and Law, Security Breaches and Attacks, Medical Privacy and Security Stories, Ethical issues in data use, Patient rights and informed consent.

Unit V
Emerging technologies such as artificial intelligence, machine learning, and block chain and their potential impact, Telemedicine and remote healthcare delivery, personalized medicine, precision medicine, and patient-centered care, Role of health informatics in global health

Textbooks
1. Hoyt, Robert E., and Ann K. Yoshihashi. Health informatics: practical guide for healthcare and information technology professionals. Lulu. com, 2014.
2. Health Informatics: An Introduction by Ramona O. Nelson and Waldo Emerson, Jr.