DETAILED SYLLABUS

FOR

MASTER OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

SEMESTER I

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

ISLAMIC UNIVERSITY OF SCIENCE AND TECHNOLOGY, KASHMIR

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 Credits:				*18*

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.

.