CO4: fine tune machine learning algorithms and evaluate models generated from data.

Syllabus:

Unit-I Introduction to Artificial Intelligence: Evolution of AI as a discipline, Definitions and approaches, Subject matter of AI, Foundations of AI, Philosophical issues, AI for all, Ethical Issues and Responsible AI.

Unit-II Introduction to Machine Learning: Hypothesis and target class, bias-variance tradeoff, Occam's razor, Approximation and estimation errors, Curse of dimensionality, dimensionality reduction, feature scaling, feature selection methods.

Unit-III Regression: Linear regression with one variable, Linear regression with multiple variables, Gradient Descent, Logistic Regression, Polynomial regression, over-fitting, regularization. performance evaluation metrics, validation methods.

Unit-IV Classification: Decision trees, Naive Bayes classifier, Perceptron, multilayer perceptron, Neural network, back-propagation Algorithm, Support Vector Machine, Kernel functions.

Unit V Evaluation: Performance evaluation metrics, ROC Curves, Validation methods, Bias-variance decomposition, Model complexity.

Unit-VI Unsupervised Learning: Clustering, distance metrics, Mixture models, Expectation Maximization, Cluster validation methods.

Readings:

1. Alpaydin, Ethem, **Introduction to machine learning,** MIT press, 2014.
2. T. M. Mitchell, Machine Learning, McGraw Hill Education, 2017.
3. Christopher, M. Bishop, **Pattern Recognition And Machine Learning**, Springer-Verlag, 2016.
4. Shai Shalev-Shwartz, Shai Ben-David, **Understanding Machine Learning: From Theory to Algorithms,** Cambridge Press, 2014.
5. Michalski, Ryszard S., Jaime G. Carbonell, and Tom M. Mitchell, eds. **Machine learning: An artificial intelligence approach**, Springer Science & Business Media, 2013.

MCSC103: INFORMATION SECURITY [3-0-1]

Course Objectives: The course aims to train the students to maintain the confidentiality, integrity and availability of data. The student learns various data encryption protocols for transmitting data over unsecured channels in a network.

Course Learning Outcomes:

CO1 To be able to describe various security issues.
CO2 To be able to implement a symmetric and asymmetric cryptographic methods.
CO3 To be able to describe the role and implementation of digital signatures.
CO4 To be able to describe security mechanisms like intrusion detection, auditing and logging.

Syllabus:

Overview of Security: Protection versus security; aspects of security– confidentiality, data integrity, availability, privacy; user authentication, access controls, Orange Book Standard.

Security Threats: Program threats, worms, viruses, Trojan horse, trap door, stack and buffer overflow; system threats- intruders; communication threats- tapping and piracy.

Computer Security Models: BLP Model, BIBA Model, HRU Model.

Cryptography: Substitution, transposition ciphers, symmetric-key algorithms: Data Encryption Standard, Advanced Encryption Standard, IDEA, Block cipher Operation, Stream Ciphers: RC-4. Public key encryption: RSA, ElGamal. Diffie-Hellman key exchange. Elliptic Curve, EC cryptography, Message Authentication code (MAC), Cryptographic hash function.

Digital signatures: ElGamal digital signature scheme , Elliptic Curve digital signature scheme, NISTdigital signature scheme.

Key Management and Distribution : Symmetric Key Distribution, X.509 Certificate public key infrastructures.

Intrusion detection and prevention.

Readings:

1. W. Stalling, **Cryptography and Network Security Principles and Practices** (7th ed.), Pearson of India, 2018.
2. A.J. Elbirt, Understanding and Applying Cryptography and Data Security, CRC Press, Taylor Francis Group, New York, 2015.
3. C. Pfleeger and SL Pfleeger, Jonathan Margulies, **Security in Computing** (5th ed.), Prentice-Hall of India, 2015
4. M. Merkow and J. Breithaupt, **Information Security: Principles and Practices**, Pearson Education, 2006.

MCSC104: MATHEMATICAL FOUNDATIONS OF COMPUTER SCIENCE [3-0-1]

Course Objectives:
This course will discuss fundamental concepts and tools in discrete mathematics with emphasis on their applications to computer science. The objectives of this course comprise of providing students knowledge of logic and boolean circuits, sets, functions, relations, deterministic and randomized algorithms. Furthermore, the students will learn analysis techniques based on counting methods, recurrence relations, trees and graphs.