School of Electrical Sciences

Curriculum and Syllabus for M.Tech. (Artificial Intelligence)

Semester –I				
SN	Course Name	Code	L-T-P	Credit
1	Mathematical Foundations of AI	CS6LXXXX	3-0-0	3
2	Data Intensive Computations	CS6LXXXX	3-0/1-0	3-4
3	Introduction to Machine Learning	CS6LXXXX	3-0/1-0	3-4
4	Artificial Intelligence Systems	CS6LXXXX	3-1-0	4
5	E1: Elective-I	CS6LXXXX	3-0/1-0	3-4
6	Computer Systems Lab-I	CS6PXXXX	0-0-3	2
7	Machine Learning and AI Lab	CS6PXXXX	0-0-2	2
8	Seminar-I	CS6PXXXX	0-0-0	2
Total Credits				22-25

Semester-II				
SN	Course Name	Code	L-T-P	Credit
1	Deep Learning	CS6LXXXX	3-0-0	3
2	High Performance Computer Architecture	CS6LXXXX	3-1-0	4
3	E2:Elective-II	CS6LXXXX	3-0/1-0	3-4
4	E3:Elective-III	CS6LXXXX	3-0/1-0	3-4
	E4:Elective-IV	CS6LXXXX	3-0/1-0	3-4
5	Deep Learning Lab	CS6PXXXX	0-0-3	2
6	Advanced ML Lab	CS6PXXXX	0-0-3	2
7	Seminar-II	CS6PXXXX	0-0-0	2
Total				22-25

Semester-III				
Sl. No	Course Name	Code	L-T-P	Credit

1	Thesis (Part-I)	CS6TXXXX	0-0-0	20
Total				20
Semester-IV				
Sl. No	Course Name	Code	L-T-P	Credit
1	Thesis (Part-II)	CS6TXXXX	0-0-0	20
Total				20

Total Credit: 84-90

List of Electives

1. Advanced Algorithms
2. Networks and Systems Security
3. Computer Vision
4. Software Testing and Verification
5. Internet of Things
6. Natural Language Processing
7. Multimedia Systems
8. Current Topics in AI and ML
9. Cloud Computing
10. Game Theory
11. Advanced Topics in AI and Architecture
12. AI in Healthcare
13. Parallel and Distributed Algorithms
14. Machine Learning in Robotics
15. Machine Learning and Cyber Security
16. Pattern Recognition
17. Software Engineering of AI systems

Compliance Report

Category	MTech Curriculum (Requirement)		Proposed MTech (CSE) Curriculum
	Subjects	Credits	Credits

1. Theory (8-10) numbers	Core (40-60%)	32-36	20-22 (6 numbers)
	Electives (40-60%)		12-16 (4 numbers)
2. Laboratories		6-8	8
3. Seminars		4	4
4. Thesis	3rd Semester	20	20
	4th Semester	20	20
Total		82-88	84-90

CORE COURSES

Subject Code: CSXXX	Name: Mathematical Foundations of AI	L-T-P: 3-0-0	Credits: 4

Syllabus:

Advanced Vector Calculus • Multivariate derivatives and chain rule • Backpropagation and automatic differentiation • Linearization and multivariate Taylor series

Advanced Linear Algebra • Eigenvalues and eigenvectors • Singular value decomposition • Matrix approximation

Continuous Optimization • Gradient descent • Constrained optimization and Lagrange multipliers • Convex Optimization, **non-linear optimization**

Models and Data • Change of variables • Empirical risk minimization • Parameter estimation • Probabilistic modelling and inference • Model selection

Basic Applications for AI systems • Linear Regression • Dimensionality Reduction with Principal Component Analysis (PCA) • Density Estimation with Gaussian Mixture Model

Logic and Deduction: Propositional Logic, Predicate Logic, Resolution Refutation, Constraint satisfaction problems

Random Processes, Markov Chain, state transition diagrams, steady state, Game theory basics

Prerequisite:

Textbooks:

1. Tsang. Foundations of constraint satisfaction, Books on Demand Publishers. Available free online.
2. Deisenroth M.P., Faisal, A.A., Ong, C.S.: Mathematics for Machine Learning. Cambridge University Press, Cambridge (2020)

Reference Books:

1. C. M. Bishop: Pattern Recognition and Machine Learning, Springer, 2006
2. **Kisor Tribedi: Probability and Statistics with Reliability, Queuing and Computer Science Applications (2nd Ed)**, Wiley.

Subject Code: CSXXX	Name: Artificial Intelligence Systems	L-T-P: 3-0-0	Credits: 4

Syllabus:

Intelligent agents and environments, End to end development of AI systems

Logic: Classical Models, Temporal Models
Problem Solving: Techniques behind DeepBlue, Watson Jeopardy, AlphaGo
Probabilistic modelling and reasoning
Decision making under uncertainty

Pattern Recognition: Learning from examples and more advanced learning techniques that contribute to most modern AI applications

Knowledge, reasoning and planning, Knowledge representation: fuzzy, temporal, beliefs, if-then rules
Introduction to Robotics, NLP and Computer vision.

Case studies: Overview of AI in automotive, Robotic, Transportation and Vision based Systems.

Prerequisite: Mathematical Logic, Discrete Mathematics

Textbooks:

1. Russell and Norvig. Artificial Intelligence: A Modern Approach, Prentice Hall, 3rd edition.
2. Koller and Friedman. Probabilistic Graphical Models: Principles and Techniques - Adaptive Computation and Machine Learning, Cambridge University Pres

Reference Books:

1. Hastie, Tibshirani, and Friedman. The elements of statistical learning. Springer. Available free online.
2. Tsang, Foundations of constraint satisfaction, Books on Demand Publishers. Available free online.

Subject Code: CSXXXX	Name: Introduction to Machine Learning	L-T-P:	Credits:

Syllabus: Introduction to Machine Learning: History of ML, AI vs. ML, Types of Learning (supervised, unsupervised, semi, weak, self, etc.). Types of Data: Tabular, Image, Video, Audio, Sequential, etc. Feature Engineering, ML approaches: Introduction to regression, classification, clustering. Regression: Linear Regression, Multiple Linear Regression, Support Vector Regression, Ridge regression. Classification: Naïve Bayes, Logistic regression, Support Vector Machine, K-nearest neighbors, Decision Tree, Random Forest. Clustering: Density-based, Distribution-based, K-means, DBSCAN, Gaussian Mixture Models, Mean-shift clustering. Advanced ML: Perceptron, Artificial Neural Network, Bayesian Network, Gradient Descent algorithm. Evaluation: Train-test split, Cross-validation, k-fold validation, stratified k-fold validation, bootstrapping, cross-entropy loss, binary cross-entropy, L1-loss, L2-loss, regularization, dropouts, confusion matrix, AUC-ROC, EER, RMS, Precision, Recall and mAP. Reinforced machine learning, Ensemble Methods, Expectation-Maximization.

ML application examples from medicine, business, image processing, sports, social media and others.

Prerequisite: Calculus, Linear Algebra, Statistics.

Textbooks:

1.Gareth James, Daniela Witten, Trevor Hastie, Robert Tibshirany, Jonathan Taylor , "An Introduction to Statistical Learning with Applications in Python," Springer, 2023.

Reference Books:

The Elements of Statistical Learning: Data Mining, Inference, and Prediction, Trevor Hastie, Robert Tibshirani, and Jerome Friedman, Springer, 2nd Edition, 2017.

Tools and Software: Python/R programming, Numpy, Tensorflow

Subject Code: CSXXXX	Name: Deep Learning	L-T-P: 3-0-0	Credits:

Syllabus: Introduction to Deep Learning: History of DL, DL vs. ML, Types of Learning (supervised, unsupervised, semi, weak, self, etc.). Linear Classifiers, Linear Machines with Hinge Loss. Optimization Techniques, Gradient Descent, Batch Optimization. Introduction to Neural Network, Multilayer Perceptron, Back Propagation Learning. Unsupervised Learning with Deep Network. Convolutional Neural Network, building blocks of CNN (activation, normalization, pooling, padding), Transfer Learning, hyper-parameter tunning, Revisiting Gradient Descent, Momentum Optimizer, RMSProp, Adam optimizer. Effective training in Deep Net- early stopping, Dropout, Batch Normalization, Instance Normalization, Group Normalization. Recent Trends in Deep Learning Architectures, Residual Network, Skip Connection Network, Fully Connected CNN, LSTM, Autoencoders, Transformers, Multi-branch CNN, Generative Networks (GAN), Recurrent Neural Nets (RNN), GRU, complex models. Classical Supervised Tasks with Deep Learning, Image Denoising, Semantic Segmentation, Object Detection, Anomaly Detection, Object tracking, optical flow estimation, etc. LSTM Networks, Generative Modeling with DL, Variational Autoencoder, Generative Adversarial Network Revisiting Gradient Descent, Momentum Optimizer. Natural language processing: word embeddings, sentiment analysis.

Prerequisite: Knowledge of Linear Algebra, Digital Signal Processing, will be helpful.

Textbooks:

1. Deep Learning - Ian Goodfelllow, Yoshua Benjio, Aaron Courville, The MIT Press, 2016.
2. Grokking Deep Learning - Andrew W. Trask, Manning Publications, 2019.

Reference Books:

3. Pattern Classification - David G. Stork, Peter E. Hart, and Richard O. Duda, 2nd Edition, Wiley, 1973.
4. Pattern Recognition, Theodoridis, S. and Koutroumbas, K. Edition 4. Academic Press, 2008.

Tools and Software: PyTorch, Keras, Tensorflow.

Laboratory Courses

Subject Code: CSXXXX	Name: Machine Learning and AI Lab	L-T-P:	Credits:

Syllabus: Python/R programming: Installation, editors, keywords, statements, arguments, decision makings, functions, exception handling, file handling, modules, and system packages (OS, Time, Math, Sys). Data and ML Libraries: Scikit-Learn, Numpy, Pandas, Matplotlib, Seaborn, SciPy. Feature Engineering: reading writing from CSV file using Pandas, Numpy, feature visualization using Matplotlib, Seaborn. Training-testing: Implementation of ML algorithms using Python/R or Scikit-Learn, SciPy. Case Studies: Spam detection, stock-price prediction, whether forecast, face recognition, digit recognition, dimension reduction using PCA, Heart disease prediction, regression using SVM, online transaction fraud detection and clustering using K-means, data construction on sequential data. Evaluation measures: ROC-AUC, TPR-FPR, Accuracy, EER. Plot using Matplotlib and Seaborn: Confusion Matrix, Scatter plot, regression line, cluster encoding, color mapping, multiplot, heatmaps.

A* algorithm for 8 puzzle, Logical deductions in Propositional and Predicate Calculus using Prolog , Robot blocks world problem, Planning algorithms

Prerequisite: Basic programming.

Textbooks:

1. Tom M. Mitchell, “Machine Learning”, Mc Graw Hill, Indian Edition, 2017.
2. Ethem Alpaydin, “Introduction to Machine Learning”, MIT Press, Fourth Edition, 2020.
3. Sebastain Raschka, “Python Machine Learning”, Packt publishing (open source).
4. M.A. Bramer, Logic Programming with PROLOG, Springer

Subject Code:	Name: Deep Learning Lab	L-T-P:	Credits:

Syllabus: Introduction to Python: Python: Installation, decision makings, functions, file handling, modules. Data and ML Libraries: Scikit-Learn, Numpy, Pandas, Matplotlib, OpenCV, Pillow. Introduction to DL libraries: PyTorch, Theano, Keras, Tensorflow. Basic image processing operations: Histogram equalization, thresholding, edge detection, data augmentation, morphological operations. Implement SVM/Softmax classifier for CIFAR-10 dataset: using KNN, multi-layer neural network. Study the effect of batch normalization and dropout in neural network classifier. Familiarization of image labelling tools for object detection, segmentation. Image segmentation using Mask RCNN, UNet, SegNet. Object detection with single-stage and two-stage detectors (Yolo, SSD, FRCNN, etc.). Image Captioning with Vanilla RNNs. Image Captioning with LSTMs. Network Visualization: Saliency maps, Class Visualization. Generative Adversarial Networks. Chatbot using bi-directional LSTMs. Video feature extraction using CNNs, optical flow estimation using feature pyramid networks. Dataset: CIFAR-100, MNIST, UCSD-Peds, ImageNet, LFW, KITTI, etc. Familiarization of cloud-based computing like Google colab.

Prerequisite: Basic Programming

Textbooks:

1. Deep Learning with Python -Francois Chollet, Manning; 1st edition, 2017.
2. Deep Learning from Scratch: Building with Python from First Principles - Seth Weidman, O′Reilly, 2019.
3. AI and Machine Learning for Coders - Laurence Moroney, O′Reilly, 2020.

Reference Books:

4. Deep Learning: A Practical Approach – Rajiv Chopra, Khanna Book Publishing; 1st edition, January 2018.

Tools and Software: Keras, PyTorch, Tensorflow, Pycharm, Colab, Anaconda.

Subject Code: CS6XXX	Name: Computer Systems Lab	L-T-P: 0-0-2	Credits: 3

Syllabus:

Object-oriented programming concepts and UML, Implementation of graph algorithms, Randomized and approximation algorithms, Numerical computing algorithms, Basics of System programming: process creation, Inter process communication (IPC), Implementation of scheduling algorithms, synchronization, shared memory and semaphore, shell programming and implementation of file management.. Prerequisite: Programming and Data Structures

Prerequisites: Programming and Data Structures

Text Books:

Reference Books:

Subject Code: CS6XXX	Name: Advanced Machine Learning Lab	L-T-P: 0-0-2	Credits: 3

Syllabus:

Lab assignments related to:

Sentiment Analysis and Opinion Mining for social media/E-commerce text, Recommendation system for E-commerce platform, Modelling in Web Data, Conversational Bots: ChatBots, Building news Summarizer, Spam Classifier of Messages, Building model for Sentence Auto-completion, **ChatGPT and LLMs**

Inferring structure from Data, Stock Market Analysis And Forecasting Using Deep Learning, Reinforcement Learning for Connect X, Image Caption Generator using CNN and LSTM, Generate Music using Neural Networks, Deep belief Networks

Prerequisites: Programming and Data Structures, Introduction to Machine Learning

Text Books:

Reference Books:

Elective Courses

Subject Code: CSXXXX	Name: Software Engineering of AI systems	L-T-P:	Credits:

Syllabus:

End to end development of AI systems, AI Design Patterns.

Data validation, Performance testing, Security testing, Regression testing and Integration testing of AI systems
Attacks based on numerical optimization or saliency maps
Testing of robustness
Coverage analysis of Neural networks, White box/ Black box testing of NNs,
Testing of Deep Neural Networks,
Mutation testing of DNN
Input space characterization, Input Prioritization
Theoretical Verification of ML algorithms: Verification of security guarantee
Statistical model checking on Neural Networks

Prerequisite: Artificial Intelligence

Textbooks:

1. Huang, X., Kwiatkowska, M., Wang, S., & Wu, M. (2016). Safety Verification of Deep Neural Networks. arXiv preprint arXiv:1610.06940.
2. Katz, G., Barrett, C., Dill, D., Julian, K., & Kochenderfer, M. (2017). Reluplex: An Efficient SMT Solver for Verifying Deep Neural Networks. arXiv preprint arXiv:1702.01135.

Reference Books:

1. Pulina, L., & Tacchella, A. (2010, July). An abstraction-refinement approach to verification of artificial neural networks. In International Conference on Computer Aided Verification (pp. 243-257). Springer Berlin Heidelberg.
2. Vapnik, V. (1998). Statistical Learning Theory, Wiley

Subject Code: CS6L031	**Name:** Game Theory	**L-T-P:** 3-0-0	**Credits:** 3

Prerequisite: Design and Analysis of Algorithms / Advanced Algorithms

Syllabus:

Introduction: Introduction to game theory, current trends and modern applications.

Non-Cooperative Game Theory: Key notions, strategic form games, extensive form games, dominant strategy equilibrium, pure strategy Nash equilibrium, mixed strategy Nash equilibrium, two player zero sum game, existence of Nash equilibrium, computation of Nash equilibrium, complexity analysis of Nash equilibrium, Bayesian games.

Mechanism Design: Introduction, social choice functions, incentive compatibility and revelation theorem, Gibbart-Satterthwaite impossibility theorem, Arrow's impossibility theorem, VCG mechanisms, Quasilinear environment, revenue equivalence theorem, optimal mechanisms and Myerson auction

Cooperative Game Theory: Correlated equilibrium, coalition games, core of coalition games, Shapley value, Benzhaf index, stable matching.

Text Books:

1. Y. Narahari. *Game Theory and Mechanism Design*. IISc Press and the World Scientific. 2014.
2. Michael Maschler, Eilan Solan, and Schmuel Zamir. *Game Theory*. Cambridge University Press, 2013
3. Roger B. Myerson. *Game Theory: Analysis of Conflict*. Harvard University Press, September 1997

Reference Books:

1. Roger B. Myerson. *Game Theory: Analysis of Conflict*. Harvard University Press, September 1997.
2. Andreu Mas-Colell, Michael D. Whinston, and Jerry R. Green. *Microeconomic Theory*. Oxford University Press, New York, 1995.
3. Martin J. Osborne, Ariel Rubinstein. *A Course in Game Theory*. The MIT Press, August 1994.
4. Philip D. Straffin, Jr. *Game Theory and Strategy.* The Mathematical Association of America, January 1993.
5. Ken Binmore, "*Fun and Games : A Text On Game Theory*", D. C. Heath & Company, 1992.
6. Paul Klemperer, *Auctions: Theory and Practice*, The Toulouse Lectures in Economics, Princeton University Press, 2004.
7. Noam Nisan, Tim Roughgarden, Eva Tardos, Vijay V. Vajirani, *Algorithmic Game Theory*, Cambridge University Press, 2007.

Subject Code: CS6L032	**Name:** Parallel and Distributed Algorithms	**L-T-P:** 3-0-0	**Credits:** 4

Prerequisite: Design and Analysis of Algorithms / Advanced Algorithms
Syllabus:

Parallel Algorithms: Parallel Programming Models: Shared-memory model (PRAM, MIMD, SIMD), network model (line, ring, mesh, hypercube), performance measurement of parallel algorithms.
Algorithm Design Techniques for PRAM Models: Balancing, divide and conquer, parallel prefix computation, pointer jumping, symmetry breaking, pipelining, accelerated cascading.

Algorithms for PRAM Models: List ranking, sorting and searching, tree algorithms, graph algorithms, string algorithms.

Algorithms for Network Models: Matrix algorithms, sorting, graph algorithms, routing, Relationship with PRAM models.
Parallel Complexity: Lower bounds for PRAM models, the complexity class NC, P-completeness.

Distributed Algorithms: Basic concepts. Models of computation: shared memory and message passing systems, synchronous and asynchronous systems.

Logical time and event ordering. Global state and snapshot algorithms, clock synchronization.

Distributed Operating Systems: Mutual exclusion, deadlock detection

Classical Algorithms: Leader election, termination detection, distributed graph algorithms.

Fault tolerance and recovery: basic concepts, fault models, agreement problems and its applications, commit protocols, voting protocols, checkpointing and recovery, reliable communication.
Security and Authentication: basic concepts, Kerberos. Resource sharing and load balancing.

Text Books:
1. Joseph F Jájá, *An Introduction to Parallel Algorithms*, Addison-Wesley, 1992.
2. Mukesh Singhal, Niranjan Shivaratri, *Advanced Concepts in Operating Systems*, McGraw-Hill.

Reference Books:
1. Michael J Quinn, *Parallel Computing: Theory and Practice*, second edition, McGraw Hill, 2002.
2. Michael J Quinn, *Parallel Programming in C with MPI and OpenMP*, first edition, McGraw Hill, 2004.
3. Ananth Grama, Anshul Gupta, George Karypis and Vipin Kumar, *Introduction to Parallel Computing*, second edition, Addison-Wesley/Pearson, 2003.
4. Nancy Lynch, *Distributed Algorithms*, Morgan Kaufmann.
5. Andrew S. Tanenbaum, *Distributed Operating Systems*, ACM Press.
6. Jie Wu, *Distributed Systems*, CRC Press.
7. Hagit Attiya, Jennifer Welch, *Distributed Computing: Fundamentals, Simulations and Advanced Topics*, McGraw-Hill.

Subject Code: CSXXXX	Name: Advanced Algorithms	L-T-P: 3-0-0	Credits:

Syllabus:

Network flow problems, Bipartite Matching, Stable marriage problem and its variations, Combinatorial Problems: Voltage and Current graphs

NP and NP-Hard problems, Polynomial reductions: Boolean satisfiability, 3-SAT, Graph colouring, Vertex cover, Hamiltonian Cycle, TSP, Set Cover, Subset Sum, Knapsack

Linear Programming: Simplex Algorithm

Space Complexity: PSPACE, PSPACE-complete, EXPTIME,
Heuristics, Approximation Algorithms
Randomized Algorithms

Prerequisite:

Textbooks:

1. J. Kleinberg, Eva Tardos, Algorithm Design, Addison Wesley
2. Cormen, Leisersson, Rivest and Stein. Introduction to Algorithms, PHI

Reference Books:

1. R.K. Ahuja. Network Flows: Theory, Algorithms and Applications, Pearson.
2. R. Motwani, P. Raghvan. Randomized Algorithms, Cambridhe University Press.
3. V.V. Vazirani, Approximation algorithms, Springer.

Subject Code: CSXXXX	Name: IoT	L-T-P: 3	Credits: 3

Syllabus:

Introduction: Introductions to IoT; various IoT systems and challenges; IoT trends;

IoT Architecture and Components: System architecture; hardware; operating systems; Sensors; scope of device drivers; edge computing; cloud-computing supports;

IoT Frameworks: ARTIK platform and usages; IFTTT platform and usages

Networks and Protocols for IoT: Sensor networks for IoT, energy conserving MAC and network layer protocols, device discovery protocols.

Emerging attributes of IoT: Artificial intelligence for IoT; Cognitive IoT; multimodal modelling; programmability; tools and platforms;

IoT Data analytics: Understanding IoT data; IoT data collection and integration; machine learning techniques for data analysis; advanced analytics; IoT analytics tools;

IoT Security and Privacy: Authentications, biometric authentications; software / applications with dynamic authentication; privacy along with security, Fluid media; privacy and security with VANET;

Case studies: IoT wearable and healthcare; industrial IoTs; Low-power considerations in IoT; and voice user interactions;

Internet of Drones: Applications in civil and military domains.

Prerequisite: None

Text Books:
1. IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things; (1st Edition); by David Hanes et. al; Cisco Press, 2017; ISBN-10: 1587144565.

Reference Books:
1.Internet of Things for Architects: Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security; By Perry Lea, ISBN-10: 1788470591; Wiley Publication, 2018.

Subject Code: CS6L023	Name: Software Testing and Verification	L-T-P: 3-0-0	Credits: 3

Syllabus: The course is about how to convince oneself that a program unit really does what it should. There are different methods for verifying programs that will be covered in this course. Testing: which has the purpose of finding errors in a program in a systematic way (terminology, coverage, unit tests, a unit test framework). Debugging which has the purpose to systematically trace and eliminate an error (control, workflow, localization, tools). Proving or formal verification: reasoning about the program in order to guarantee correctness (formal specifications (pre-/ postconditions, invariants), automatic test case generation, formal verification (logics, tool support)). Verifying a program only makes sense if we can precisely specify what the program is supposed to do. Many specifications are written in natural language which might lead to imprecision and misunderstandings. In the course you will learn how to use precise methods for specifying functional requirements. Such precise specifications will then be our basis for the verification of programs. But they will also be useful to automatize the generation of test cases. Throughout, the course is concerned with imperative programs in general, and object-oriented programs in particular.

Prerequisite: NONE

Text Books:

1.Introduction to Software Testing by Paul Ammann, Jeff Offutt, 2nd Edition, 2016, Cambridge University Press
2. The Art of Software Testing, 3rd Edition by Glenford J Myers, 2015, Wiley

Reference Books:

1. Why Programs Fail: A Guide to Systematic Debugging by Andreas Zeller, 2nd Edition
2. The Science of Programming by David Gries. Springer

Subject Code: CSXXXX	Name: Machine Learning and Cyber Security	L-T-P: 3-0-0	Credits: 3

Syllabus:

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.

Introduction to Cyber Security: Basic Cyber Security Concepts, layers of security, Vulnerability, threat, Harmful acts, Internet Governance – Challenges and Constraints, Computer Criminals, Security Models, Cyber Crime, Cyber terrorism, Cyber Espionage, etc.,

Cybercrime: Mobile and Wireless Devices: Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication service Security, Attacks on Mobile/Cell Phones

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

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

Artificial Intelligence in Cyber Security: Model Stealing & Watermarking, Network Traffic Analysis, Malware Analysis

Prerequisite: Introduction to Machine Learning

Text Books:

1. Artificial Intelligence and Data Mining Approaches in Security Frameworks Editor(s):Neeraj Bhargava, Ritu Bhargava, Pramod Singh Rathore, Rashmi Agrawal, 2021.
2. Tsai, Jeffrey JP, and S. Yu Philip, eds. Machine learning in cyber trust: security, privacy, and reliability. Springer Science & Business Media, 2009.

Reference Books:

1. Nina Godbole and Sunit Belpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley
2. B. B. Gupta, D. P. Agrawal, Haoxiang Wang, Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335, 2018.
3. Russell, S. and Norvig, P, Artificial Intelligence: A Modern Approach, Third Edition, PrenticeHall, 2010.
4. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRC Press. 2. Introduction to Cyber Security, Chwan-Hwa(john) Wu,J. David Irwin, CRC Press T&F Group.
5. Gupta, Brij B., and Quan Z. Sheng, eds. Machine learning for computer and cyber security: principle, algorithms, and practices. CRC Press, 2019.
6. Machine Learning: A Probabilistic Perspective, Kevin P Murphy, MIT Press.

Subject Code: CS6XXX	**Name: Data Intensive Computing**	L-T-P: 3-0-0	Credits: 3

Syllabus:

Data Warehouse Architecture – DBMS Schemas for Decision Support – Data Extraction, Cleanup, and Transformation Tools –Metadata – reporting – Query tools and Applications – Online Analytical Processing (OLAP) – OLAP and Multidimensional Data Analysis.

Storage requirements of big data, organization of big data repositories such as Google File System (GFS) semantic organization of data, data-intensive programming models such as MapReduce, fault-tolerance, privacy, security and performance, services-based cloud computing middleware, intelligence discovery methods, and scalable analytics and visualization. This course has three majors goals: (i) understand data-intensive computing, (ii) study, design and develop solutions using data-intensive computing models such as MapReduce and (iii) focus on methods for scalability using the cloud computing infrastructures such as Google App Engine (GAE), Amazon Elastic Compute Cloud (EC2), and Windows Azure. On completion of this course students will be able to analyze, design, and implement effective solutions for data-intensive applications with very large scale data sets.

Introduction to MongoDB, guthub, Hive, Tableau and Hadoop

Security issues in Data bases: Access Control Models, Role based Access Control, Bell-Lapadula Model, SQL Injection

(Based on the syllabus of University NY at Buffalo)

Prerequisite: Database Systems

Text Books:

1. Barrie Sosinsky, Cloud Computing Bible, Wiley India. 2011
2. S. Bradshaw, E. Brazil, K. hodorow. MongoDB: The Definitive Guide, O Reilly, 2019
3. G. K. Gupta “Introduction to Data Mining with Case Studies”, Easter Economy Edition, Prentice Hall of India, 2006.

And Research papers.

Reference Books:

1. I. Gorton, DK Gracio (Editors). Data Intensive Computing: Architectures, Algorithms and Applications, Cambridge University Press

Subject Code: CS6XXX	Name: Networks and System Security	L-T-P: 3-0-0	Credits: 3

Syllabus:

Foundations of Information Security – CIA, Security Goals, Authenticity, Trust Management, Symmetric Key Cryptography – RC4, DES, AES, Asymmetric Key Cryptography – RSA, Elliptic Curve, Diffie Hellman, Perfect Secrecy, Cryptographic Hash

Network Security – IP spoofing, ARP Poisoning, Session Hijacking, SYN Flooding, DoS, Key Distribution, Access Control, Transport-Level Security (HTTPS, SSH), Wireless Network Security, Electronic Mail (Email) Security, Internet Protocol Security (IPSec), Virtual Private Network (VPN), Firewall, Network Intrusion Detection

System Security – Malware, Program Analysis, Buffer Overflow, Penetration Testing, Embedded System and Hardware Security

Security of Evolving Technologies - Software-Defined Networking Security, P2P Security, Cloud Security, Adversarial Machine Learning, Security of Cyber-Physical Systems (such as Smart Grid), Anonymous Communication Networks (such as Tor), Peer-to-Peer Communication and Payments (such as Bitcoin)

Prerequisite: None

Text Books:

1. Cryptography and Network Security: Principles and Practice, 6th Edition, William Stallings, 2014, Pearson, ISBN13:9780133354690.

2.Cryptography and Network Security, Forouzan and Mukhopadhyay, 3rd Edition, PHI.

3.Cryptography: Theory and Practices, Stinson and Patterson, 4th Edition CRC Press

Reference Books:

1.Network Security: Private Communications in a Public World, M. Speciner, R. Perlman, C. Kaufman, Prentice Hall, 2002.

2. Web Resource: A Graduate Course on Applied Cryptography Dan Boneh and Victor Soup https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup_0_4.pdf

Subject Code: CS6XXX	Name: Cloud Computing	L-T-P: 3-0-0	Credits: 3

Syllabus:
Models and architectures,

Virtualization: Virtualization Techniques, Hardware assisted CPU virtualization, Full virtualization, Para virtualization, Memory virtualization, I/O virtualization

Cloud Platforms: AWS, Azure, Google Cloud

Programming Models: MapReduce, Spark, GraphLab and Samza

VM live migration, VM check pointing and cloning, Containers

Cloud storage: Dynamo, BigTable, Haystack, Memcache

AI in Cloud: Designing and implementing machine learning models using cloud services, Google Cloud ML Machines, Azure Machine Learning, Machine learning on streaming data using cloud services, ML solutions on Cloud platforms, Optimization and of ML models on Cloud platforms,

Cloud infrastructure and security, Securing Cloud Applications

Prerequisite: None

Text Books:

1. Barrie Sosinsky, Cloud Computing Bible, Wiley India.
2. C. Korner, M. Alsdorf. Mastering Azure Machine Learning, Packt Publishing.
3. J.R. Vacca, Could Computing Security: Foundations and Challenges, CRC Press, 2020.

And Research papers

Reference Books:

1 Introduction to AWS Security, docs. aws.amazon.com

Subject Code: CS6XXX	Name: Machine Learning for Robotics	L-T-P: 3-0-0	Credits: 3

Syllabus:
Reading and Processing of Robotic Data, simulation techniques to give robots an artificial personality, Object recognition using neural networks and supervised learning techniques

Picking up of objects using genetic algorithms for manipulation

Teach a robot to listen using NLP via an expert system

Machine learning and computer vision to teach a robot how to avoid obstacles

Path planning and search algorithms to enhance robot functions; Obstacle detection and avoidance

(Course focus will be on AI aspects and programming of Robotic systems and will be accompanied by the Robotics Lab course)

Prerequisites: Artificial Intelligent Systems

Text Books:
Francis X. Govers . Artificial Intelligence for Robotics: Build intelligent robots that perform human tasks using AI techniques, Packt Publishing, 2018

Subject Code: CS6XXX	Name: : High Performance Computer Architecture	L-T-P: 3-0-0	Credits: 3

Syllabus:
Fundamentals of quantitative design and analysis, memory hierarchy design, instruction level parallelism and CPU pipelines, data level parallelism – SIMD and GPU computing, thread level parallelism - multiprocessors and parallel computing, warehouse computing - data center architecture, performance/power/cost optimizations, introduction to domain specific architectures for AI and ML applications.

Graph parallelization, numeric computing, Mapping of parallel algorithms to parallel architectures.

Prerequisites: : Digital logic design

Text Books:
John Hennessy and David Patterson. Computer Architecture: A Quantitative Approach, Morgan Kaufman, sixth edition.

Reference Books: Mostly Research papers

Subject Code: CS6XXX	Name: AI in Healthcare	L-T-P: 3-0-0	Credits: 3

Syllabus:

Hospital day to day activities Work flow, Hospital Information Management System, healthcare without and with AI, Benefits of AI, Risks and Challenges of using AI in medicine.

Collection/Curing/Storage of Medical data: Different types and formats of data in Radiology – X-Rays, MRI, CT-Scans, PetCT, Pathology, Clinical Data-Audio and Visual Recordings. Tools to collect, curate and store this data.

Five to Six AI Use cases in Medicine with ML modelling examples in areas such as Cancer, pulmonary diseases, opthalmology, Psychiatry, Haematology and others.

Connecting everything together: Class project on how to use an AI model using existing, open source models/tools

Clinical validation of AI tools, Exercises on how to validate the correctness of an AI model using Chest X-Rays or other images as an example.

One class project to implement a machine learning model for any area in medicine, using TensorFlow or a similar development platform.

Prerequisites: Introduction to Machine Learning

Text Books:

1. Parag Mahajan, "Artificial Intelligence in Healthcare," MedMantra, LLC; 3rd edition, 2021.

2. A Shaban-Nejad, Martin Michalowski, David Buckeridge, "Explainable AI in Healthcare and Medicine, Springer 2021

Reference Books:

Subject Code: CS6XXX	Name: : High Performance Computer Architecture	L-T-P: 3-0-0	Credits: 3

Syllabus:
Fundamentals of quantitative design and analysis, memory hierarchy design, instruction level parallelism and CPU pipelines, data level parallelism – SIMD and GPU computing, thread level parallelism - multiprocessors and parallel computing, warehouse computing - data center architecture, performance/power/cost optimizations, introduction to domain specific architectures for AI and ML applications.

Graph parallelization, numeric computing, Mapping of parallel algorithms to parallel architectures.

Prerequisites: : Digital logic design

Text Books:
John Hennessy and David Patterson. Computer Architecture: A Quantitative Approach, Morgan Kaufman, sixth edition.

Reference Books:

Subject Code: CS6XXX	Name: Pattern Recognition	L-T-P: 3-0-0	Credits: 3

Syllabus:

Introduction to Pattern Recognition, Feature Detection, Classification, Review of Probability Theory, Conditional Probability and Bayes Rule, Random Vectors, Expectation, Correlation, Covariance, Review of Linear Algebra, Linear Transformations, Decision Theory, ROC Curves, Likelihood Ratio Test, Linear and Quadratic Discriminants, Fisher Discriminant, Sufficient Statistics, Coping with Missing or Noisy Features, Template-based Recognition, Feature Extraction, Eigenvector and Multilinear Analysis, Training Methods, Maximum Likelihood and Bayesian Parameter Estimation, Linear Discriminant/Perceptron Learning, Optimization by Gradient Descent, Support Vector Machines, K-Nearest-Neighbor Classification, Non-parametric Classification, Density Estimation, Parzen Estimation, Unsupervised Learning, Clustering, Vector Quantization, K-means, Mixture Modeling, Expectation-Maximization, Hidden Markov Models, Viterbi Algorithm, Baum-Welch Algorithm, Linear Dynamical Systems, Kalman Filtering, Bayesian Networks, Decision Trees, Multi-layer Perceptrons, Reinforcement Learning with Human Interaction, Genetic Algorithms, Combination of Multiple Classifiers "Committee Machines"

Pre-requisite

Text Books:

Duda, R.O., Hart, P.E., and Stork, D.G. Pattern Classification. Wiley-Interscience. 2nd Edition. 2001

References:

Bishop, C. M. Pattern Recognition and Machine Learning. Springer. 2007. •
Marsland, S. Machine Learning: An Algorithmic Perspective. CRC Press. 2009. (Also uses Python.) •
Theodoridis, S. and Koutroumbas, K. Pattern Recognition. Edition 4. Academic Press, 2008.

Subject Code: CS6XXX	Name: Computer Vision	L-T-P: 3-0-0	Credits: 3

Syllabus:

Digital Image Processing: Image Formation, Image Filtering, Edge Detection, Principal Component Analysis, Corner Detection, SIFT, Applications: Large Scale Image Search

Geometric Techniques in Computer Vision: Image Transformations, Camera Projections, Camera Calibration, Depth from Stereo, Two View Structure from Motion, Object Tracking,

Machine Learning for Computer Vision: Introduction to Machine Learning, Image Classification, Object Detection, Semantic Segmentation

Pre-requiaite: Introduction to Machine Learning

Textbooks

1. Forsyth and Ponce, "Computer Vision: A Modern Approach", Pearson, 2015.
2. Hartley and isserman, "Multiple View Geometry in Computer Vision", Cambridge university press, 2004
3. There is no textbook for the third part and will be taught on the basis of recent research papers.

References:

Research papers

(Based on the syllabus of IIT Delhi)