PES UNIVERSITY

Ph.D. / MTech by Research course work syllabus

Computer Science and Engineering

List of courses

#	Course Code	Course Title
1	UE24CS641A	Computer Systems for Programmers
2	UE24CS642A	Advanced Data Structures
3	UE24CS643A	Scalable Computing
4	UE24CS644A	Stochastic models and Machine Learning
5	UE24CS645A	Cyber Security Essentials
6	UE24CS641B	Topics in Advanced Algorithms
7	UE24CS642B	Distributed Computing
8	UE24CS643BA1	Million Way Parallelism
9	UE24CS643BA2	Speech and Natural Language Processing
10	UE24CS643BA3	Topics in Computer and Network Security
11	UE24CS644BB1	Advances in Cloud Computing
12	UE24CS644BB2	Virtual Reality and its applications
13	UE24CS644BB3	Software Security
14	UE24CS645BC1	Advanced Big Data Analytics
15	UE24CS645BC2	Deep Learning Theory and Practices
16	UE24CS645BC3	Cryptography
17	UE21CS841A	Computer Vision
18	UE21CS842A	Data Mining
19	UE21CS843A	Natural Language Processing
20	UE21CS844A	IOT Architecture and Protocols
21	UE21CS845A	Fundamentals of IOT And Cryptographic Security
22	UE22CS841A	Geomatics Engineering
23	UE22CS842A	IOT For Connected Healthcare I
24	UE23CS841A	Health Digital Twin and Extended Reality
25	UE23CS842A	IOT For Connected Healthcare II

UE24CS641A: Computer Systems for Programmers

This course is an in-depth analysis of the programming interface to the hardware subsystems/mapping of contemporary processor architectures-based computing system. This course provides an end-to-end picture in sufficient advanced detail of Instruction Set Architecture, pipelining and program construct mapping to memory hierarchy.

Course Objectives:

- Introduce concepts of basic processor architecture and its design.
- Understand the concepts of pipeline architecture and hazards.
- Understand the concepts of linking, from traditional static linking, to dynamic linking of shared libraries at load time, to dynamic linking of shared libraries at run time.
- Describes the memory hierarchy, cache memory and its optimization and various benefits of a virtual memory system.

Course Outcomes:

- At the end of the course the student will be able to
- Trace the execution of a program with respect to modern processor architecture fundamentals, Caching.
- Design and implement Instruction Set Simulators for novel processor architectures.
- Write and debug complex programs.

Course Content:

Unit 1: Introduction to computer systems: Compilation system, Processor functioning, Caches, Storage devices, Networks, information storage, Processes, Threads and Concurrency, Parallelism, Number representations. Machine level representation of programs.

14 Hours

Unit 2:Processor architecture: Instruction set architecture logic design, Clocking, Pipelining, Data hazards, Exception handling, Simulators.

14 Hours

Unit 3: Linking

Compiler drivers, Static linking, Object files formats, re-locatable object files, Symbol tables, Symbol resolution, Relocation, Dynamic linking, Shared libraries, Loading executable object files, Position independent code.

14 Hours

Unit 4: Memory Hierarchy: Storage technologies, locality of reference, cache memories. Impact of caches on program performance**. Virtual Memory**: Page tables, Locality, Address translation, memory mapping, Dynamic memory allocation, Garbage collection, and Common memory related bugs.

14 Hours

Tools/Languages: C/C++/Python/Java based IDEs and Instruction Set Simulators for Pipelined Multicore processors.

Text Book(s):

1: "Computer Systems: A Programmer's Perspective", Randal Bryant and David O' Halloran, Prentice Hall, 3rd Edition, 2011.

Reference Book(s):

1. Computer Architecture: A Quantitative Approach", Hennessey and Patterson, MK publishers, 6thEdition, 2011.

UE24CS642A: Advanced Data Structures

Data Structures play a central role in modern computer science. Data Structures are the essential building blocks in building efficient algorithms. The course on Advanced Data Structures includes review of basic data structures like stacks, queues and lists. The course also includes study of complex data structures, analysis of complex data structures and their applications.

Course Objectives:

- Appreciate the impact of Data Structures on Algorithms, Program Design and Program Performance.
- Understand and apply Amortized Analysis on Data Structures, including Binary search trees, Mergeable Heaps and Dynamic Tables.
- Understand advanced ADTs with Interface and Implementation separation.
- Understand State Space search and Spatial Data Structures with R-Trees.

Course Outcomes:

At the end of the course the student will be able to

- Demonstrate the notion of Abstract Data Types (ADT) & illustrate the relation between Data Structure operations and Amortized Complexity analysis.
- How to Analyze Iterated Lists and variations thereof and demonstrate tree
- data structures and how to balance them, for specific access needsImplement different Heaps and B-Tree variations.
- Analyze and implement spatial data implementations and their search.

Course Content:

Unit 1: Complexity Analysis: Complexity, Amortized Analysis, Abstract Data Types (ADT), List Asymptotic Complexity Notations, Amortized Complexity Analysis of Stacks, Binary Counters, and Dynamic Tables, Concept of interface and implementation, Array as an ADT: Different types of Array Implementations. List Interface & List implementations, Concept of Iterator: Operations on Lists and Arrays – traverse, search, replace, reverse, copy, Doubly Linked List.

14 Hours

Unit 2: Linked List Variations, Graphs: Skip List: interface and implementation, Multilist: Sparse Matrices, Graphs-Representation, Graph Algorithms: elementary algorithms, Bellman Ford, Johnson's algorithm for sparse graphs, Graph Isomorphism, State space search techniques, Branch and Bound techniques

14 Hours

Unit 3: Trees and Queue: Tree: Basics, Self-Balancing Binary Search Trees, Trie: Prefix and Suffix trees, Treaps, Double Ended Queue.

14 Hours

Unit 4: Priority Queue and Combination of Data Structures: Priority Queues: Leftist Heaps, Skewed Heaps, Binomial Heaps, Fibonacci Heaps, Greedy method, Introduction to Spatio-Temporal Data structures and R-Trees, Log structured Merge Trees.

14 Hours

Tools/Languages: C, C++, Java or Python Programming Languages

Text Book(s):

1: "Introduction to Algorithms", T. H Cormen, C E Leiserson, R L Rivest and C Stein, MIT Press, 4th Edition, 2022.

2: "Abstract Data Types: Specifications, Implementations, and Applications", Nell Dale, Henry M. Walker, Jones & Bartlett Learning, 1996.

3: "Data Structures and Algorithm Analysis in C++", Mark Allen Weiss, Pearson, 4th Edition, 2014.

Reference Book(s):

1: "Spatial Statistics and Spatio-Temporal Data: Covariance Functions and Directional Properties", Michael Sherman, Wiley, 2010.

2: "Data Structures and Algorithms", Alfred V. Aho, Jeffrey D. Ullman, Pearson, 1983.

UE24CS643A: Scalable Computing

With an increase in the amount of data and need for remote computation due to cloud computing, this course intends to introduce the students to the business needs that have driven the change and then the underlying technologies and principles of computing at scale.

Course Objectives:

- Introduce the basic principles of computing at scale and differentiate between scale up and scale out.
- Understand Cloud service models, programming models and distributed storage and how they impact the

  design of scalable systems.
- Understand Orchestration and DevOps in Cloud Computing
- Introduce case studies of scalability from Cloud computing and Big Data and how the two relate to each other.

Course Outcomes:

At the end of the course the student will be able to

- Analyze and estimate trade-offs in computing at scale.
- Evaluate Service- oriented technologies and distributed storage architecture and their potential for transformation of business.
- Demonstrate use of Kubernetes, Azure and DevOps for developing applications at scale.
- Demonstrate development of Cloud/Hadoop applications.

Course Content:

Unit 1 : Systems Modeling, Clustering and SOA: Operating systems concepts review, Scalable computing over the internet, Technologies for network based systems, system models for distributed and cloud computing, Software environments for distributed systems, performance metrics, Services and SOA, REST,RPC .

14 Hours

Unit 2: Cloud Platform Architectures: Cloud computing and service models – IaaS, PaaS, SaaS, Architectural design, Programming models – IaaS, Master slave, p2p and overlay networks, Distributed Storage Case study: AWS/Open stack .

14 Hours

Unit 3: Programming Models: PaaS Models, Messaging Oriented Middleware, Microservices model - performance, Orchestration, Continuous integration, DevOps. Case Study: Kubernetes, Azure

14 Hours

Unit 4: Big Data Programming models: Introduction, Distributed File systems, HDFS/GFS, Map Reduce Programming Model, Spark Case Study: Netflix/Uber

14 Hours

Tools/Languages: AWS, PostMan, Flask, Docker, Kubernetes, Hadoop.

Text Book(s):

1: “Distributed and Cloud Computing: From Parallel Processing to Internet of Things”, Kai Hwang, Jack Dongarra and Geoffrey Fox, 1st Edition, 2013, Morgan Kaufmann.

Reference Book(s):

1. Dan C. Marinescu - Cloud Computing Theory and Practice-Elsevier Inc. Morgan Kaufmann (2022) Third Edition 2: “Hadoop: The Definitive Guide, Tom White”, 4th Edition, O‟Reilly, 2015.

3: Cloud Native DevOps with Kubernetes, Justin Domingus and John Arundel, O‟Reilly, 2019.

4. “Moving to the clouds: Developing Apps in the new world of cloud computing”, Dinkar Sitaram and Geetha Manjunath, Syngress, 2011.

UE24CS644A : Stochastic Models and Machine Learning

Machine Learning (ML) surrounds us today: in phones that respond to voice commands, programs that beat humans at Chess and Go, robots that assist surgeries, vehicles that drive in urban traffic, and systems that recommend products to customers on e-commerce platforms. This course aims to familiarise students with the breadth of modern ML, to impart an understanding of the dramatic surge of ML in the last decade, and to foster an appreciation for the distinctive role that ML can play in shaping the future of our society.

Course Objectives:

- Understand the basics of concept learning and decision trees.
- Understand neural networks and SVM.
- Understand Stochastic model for learning and genetic algorithms.
- Understand Unsupervised Learning models and introduce deep learning models.

Course Outcomes:

At the end of the course the student will be able to,

- Acquire thorough understanding of concept learning & decision trees.
- Apply Ensemble methods and neural networks to solve problems
- Acquire thorough undersanding of stocastic model for learning.
- Apply association rule mining for frequent item set analysis and apply deep learning models to solve real world problems.

Course Content:

Unit 1: Concept Learning and Decision Trees: Defining a Machine Learning problem, Version Spaces and Candidate Elimination Algorithm and it's Inductive Bias representation, Algorithm, Hypothesis Space Search, Inductive Bias and Issues, Performance metrics.

14 Hours

Unit 2: Ensemble Learning, ANN & SVM: Bagging and Boosting, Random Forest, Perceptrons, Gradient Descent, Back propagation, Neural Nets, Support Vector Machines (SVM).

14 Hours

Unit 3: Stochastic Models for Learning, unsupervised Learning: Bayesian Learning, Bayes Classifiers, Belief Networks, Bayesian Estimation, Expectation Maximisation (EM), Hidden Markov Models, Genetic Algorithms, Clustering, Instance based Learning.

14 Hours

Unit 4: Frequent itemset mining, Dimensionality reduction, Introduction to Deep Learning: Frequent Item Set Analysis, and FP-Growth Algorithm. Learning Complexity and Dimensionality Reduction: PAC models, Sample Complexity, Principal Component Analysis and Singular Value Decomposition, Introduction to Deep Learning, Introduction to Convolution operation & CNN, Introduction to RNN, Variants of RNN, LSTM, GRU.

14 Hours

Tools/Languages: Python 3.5 or above, Tensor flow 2.0 using Keras API.

Text Book:

1: "Machine Learning", Tom Mitchell, McGraw Hill Education (India), 2013.

Reference Books:

1:"Pattern Recognition and Machine Learning", Christopher Bishop, Springer 2nd Printing, 2011. 2:"Introduction to Machine Learning", Ethem Alpaydin, Prentice Hall (India), 3rd Edition, 2017 3: "Machine Learning in Action", Peter Harrington, Dream Tech Press (India), 2012.

UE24CS645A : Cyber Security Essentials

This course will cover the essentials of Cyber security, and students will learn about the characteristics of security principles, technologies, and procedures to secure networks, software and other assets of an organization. They will also gain an insight into Risk Management, Incident Management, Cryptography, Operations Security, Digital Forensics etc.

Course Objectives:

- To provide background information and overall view of Cyber security.
- To understand and implement secure network designs such as Firewalls, IDS, IPS, SIEM, etc.
- To analyze potential indicators associated with web application attacks. To review the basics of cryptographic concepts, use cases and limitations.
- To understand the basics of Blockchain and Digital forensics.

Course Outcomes:

At the end of this course, the students will be able to:

- Compare and contrast threats, attacks, and its indicators.
- Identify the security requirements for a network zone and determine appropriate technology.
- Classify attacks and summarize coding best practices against application attacks. Explain how cryptosystems are used to provide various principles of cyber security.
- To apply the concepts to analysis of cryptocurrency and in the field of forensics – system/memory.

Course Contents:

Unit 1: Introduction to Cyber Security and Linux Basics: CIA principles, Vulnerability, Threat and Risk, Anatomy of an Attack, Attack Landscape, Real-life Cyber-attacks, Security vs. Privacy, Security Cornerstones, Cyber security Framework, Security Mindset, Security Policy and Culture, Security Pillars, Security Principles, Cyber security best practices: Strong password, Social engineering techniques. **Basics of Linux for Security** : Linux file system, Important configuration files, Users & Permissions, Files & Permissions - SUID, SGID, Adding & removing users, locating things, grep, Environment Variables, Logging, Automated Scheduling, Shell Scripting.

14 Hours

Unit-2 Network Security and Software security:**Network Security:** Introduction to Basics of Network Security : NAT, Socket Programming using python, Packet Construction inside kernel , packet sending tools (PCAP Files). Basics of Wireshark, Scapy. **Software security:** Introduction to Secure Programming , Secure Programming in C, Attack vectors in Programming languages, Memory-based Vulnerability, Buffer Overflow Attacks.

14 Hours

Unit-3 Basics of Web Security and Cryptography: Web security basics : Fundamentals of OS, Memory Layout of a program, Architecture, HTML, CSS, Dynamic Content - Javascript, Browser server communication, Types of HTTP Requests - GET, POST, HTTPS, Cookies, Sandboxing Javascript, Ajax example, Attacks to Web, SQLI, XSS, CSRF. **Cryptography** : Definition, Terminology, History, Goal and Services, Classical Cryptography, Modern Cryptography. Types of Cryptography : Symmetric Key Cryptography, Asymmetric Key Cryptography, Hash Function. Applications of Cryptography : Steganography, Digital Signatures.

14 Hours

Unit-4 Blockchain and Digital Forensics: Blockchain: Introduction to block chain, Types of blockchain, Blockchain use cases, basic terminologies. **Digital Forensics**:Introduction to digital forensics, Digital forensic goals, Digital forensics categories and Challenges, Forensics readiness, Digital evidences,Digital forensics examination process(life cycle), Incident Response: Introduction and understanding ,Attack Lifecycle, Essential Technical Concepts. Case Study on Incident Response.

14 Hours

Proposed Labs :

1: Learn the meaning of Plagiarism.

2: Use Hashcat - password recovery tool pre-installed in kali linux to crack password hashes using various hashing algorithms and a variety of attack modes.

3: Learn the basics of network security and perform basic packet sniffing and spoofing using Scapy. 4: Introduction to Wireshark and PCAP analysis.

5: Write appropriate ufw rules to reject traffic to a website. Evade ufw firewall using SSH tunnel. 6: Web Pen Testing - SQL Injection, XSS, CSRF

7: Write a shell script to create a keylogger. 8: Crypto by hand - classical ciphers

9: Metamask wallet creation and etherscan account verification.

10: Acquiring and Analysis Digital Evidence Using FTK and Autopsy Tools

Textbook(s) :

1:“Computer Security: Principles and Practice”, William Stallings and Lawrie Brown, Pearson Education, 3rd Edition, 2010.

Reference Book (s):

1:“Computer & Internet Security: A Hands-on Approach”, Wenliang Du, 2nd Edition, 2019.

2: “The Official Comp TIA Security+ Student Guide (Exam SY0-601)”, CompTIA, Course Edition 1.0, 2020.

3: “Cryptography and Network Security”, Behrouz A.Foruzan, 3rd Edition, Tata McGraw Hill, 2017.

UE24CS641B : Topics in Advanced Algorithms

Course Objectives:

- Enable the learner with Growth of Functions, Recurrences NP completeness, Computational Geometry Convex Hull Algorithms
- Hone the problem solving skills of the learner by introducing them to Flow Networks, Bipartite Matching and Polynomials & DFT/FFT
- Introduce the learner to Number Theoretic Algorithms and String Matching Algorithms.
- Enable the learner with of Randomized, Dynamic Programming and Approximation Algorithms

Program Outcomes:

At the end of this course, the student will be able to:

- Perform Asymptotic Analysis and Estimate Algorithm Complexity
- Implement Max Flow and FFT Algorithms.
- Apply String Matching Algorithms to solve string related problems.Apply Number Theoretic concepts in designing Cryptographic Algorithms
- Solve complex problems using Dynamic Programming, Randomized Algorithms and Approximation Algorithms.

Pre-Requisite: UE23CS642A – Advanced Data Structures

Course Content:

Unit 1: Complexity Notations , NP Reductions, Computational Geometry: Asymptotic Notations, Recurrences and Solution of Recurrence equations- The Substitution method, The Recurrence tree method, The Master method,.NP-Completeness, NP Reductions, Computational Geometry Algorithms

14 Hours

Unit 2: Maximum Flow, Bi-Partite Matching, Polynomials and FFT: Flow Networks, The Ford-Fulkerson method, The Edmonds-Karp algorithm, Maximum Bi-Partite Matching, Polynomials and FFT: Representation of Polynomials, Efficient Polynomial Multiplication, DFT and FFT, Efficient Implementation of FFT.

14 Hours

Unit 3: Number Theoretic & String Matching Algorithms: Elementary notions; GCD, Modular Arithmetic, Solving modular linear equations, Modular Inverse, The Chinese remainder theorem, Powers of an element; RSA cryptosystem; Primality testing; Integer factorization. String Matching: Naïve Matcher, Rabin–Karp, String matching with Finite State Automata, and Knuth–Morris–Pratt, Boyer–Moore Algorithms

14 Hours

Unit 4: Randomized, Dynamic Programming & Appro1ximation Algorithms: Probabilistic Analysis, Randomized Algorithms: Indicator random variables,Hiring Problem, Elements of Dynamic Programming, Problems - Coin- Row, Rod-Cutting, Matrix-Chain Multiplication, Longest Common Subsequence. Approximation Algorithms: Vertex Cover Problem, TSP, The Subset Sum Problem.

14 Hours

Text Book:

: "Introduction to Algorithms", T H Cormen, C E Leiserson, R L Rivest and C Stein, PHI, 3rd Edition.

Reference Books:

1: "The Algorithm Manual", Steven Skiena, Springer, ISBN: 9788184898651.

2: "Randomized Algorithms", R Motwani and P Raghavan, Cambridge University Press 2011 edition.

UE24CS642B : Distributed Computing

Distributed computing deals with all forms of computing, information access, and information exchange across multiple processing platforms connected by computer networks. Design of distributed computing systems is a complex task. It requires a solid understanding of the design issues and an in depth understanding of the theoretical and practical aspects of their solutions. This course covers the fundamental principles and models underlying the theory, algorithms, and systems aspects of distributed computing.

Course Objectives:

- Expose students to both the abstractions and details of the file system.
- Introduce concepts related to distribute computing systems.
- To focus on performance and flexibility issues related to systems design decisions.
- To prepare students for an industrial programming environment.

Course Outcomes:

At the end of the course student will be able to,

- Apply knowledge of distributed systems techniques and methodologies.
- Explain the design and development of distributed computing and distributed computing applications.
- Use the application of fundamental Computer Science methods and algorithms in the development of distributed computing and distributed computing applications.
- Discuss the design and testing of a large software system, and to be able to communicate that design to

  others.

Course Content:

Unit 1: Introduction to Distributed Computing: Motivation, Multiprocessor Vs Multicomputer Systems, Distributed Communication models: Remote Procedure Call, Publish/Subscribe model, Message Queues etc., Design issues and Challenges for build distribute computing System. Logical time: Scalar time, Vector time, Implementation of Logical and Vector clocks.

14 Hours

Unit 2: Global snapshot: Snapshot algorithms for FIFO/ Non FIFO channels. Terminology and Basic algorithms: Classifications and basic concepts, Elementary graph algorithms, Synchronizers, Maximal Independent set, connected dominating set. Message ordering and group communication: Message ordering Paradigms, Group communication, Application level multicast.

14 Hours

Unit 3: Distributed Mutual Exclusion

Assertion based and Token based Mutual exclusion. Consensus and Agreement Protocols: Agreement in failure free and systems with failures, wait-free shared memory consensus in asynchronous systems.

14 Hours

Unit 4: Self-Stabilization: Designing self-stabilizing systems, self stabilizing distributed spanning tree, probabilistic self stabilizing leader election algorithm, self-stabilization as a solution to fault tolerance. Peer-to-Peer computing and Overlay graphs: Data indexing and overlays, unstructured and structured overlays: Bit Torrent, Tor, Bit coin, CHORD overlay, Internet graphs, Small world networks, Scale free networks, and Evolving networks.

14 Hours

Unit 5: Cluster Computing: Cluster computers and MPP architectures, Cluster job and resource management. Grid Computing: Grid architecture and service modelling, Grid resource management. Internet of Things: IoT for Ubiquitous computing, RFID, Sensors and Zig Bee technologies, Applications of IoT (smart buildings, cyber-physical systems), graph theoretic analysis of social networks, Face book, and Twitter case studies.

12 Hours

Tools / Languages: Wireshark / C compiler with Network Libraries.

Text Book(s):

1: “Distributed Computing: Principles, Algorithms, and Systems”, Ajay D. Kshemkalyani, MukeshSinghal , Cambridge University Press, 2008 (Reprint 2013).

Reference Book(s):

1: “Distributed and Cloud Computing: From Parallel processing to the Internet of Things”, Kai Hwang, Geoffrey C. Fox, and Jack J. Dongarra Morgan Kaufmann, 2012 Elsevier Inc.

2: “P2P Networking and Applications”, John F. Buford, Heather Yu, and Eng K. Lua,Morgan Kaufmann, 2009 Elsevier Inc.

3: “Grid Computing”, Joshy Joseph, and CraifFellenstein,IBM Press, Pearson education, 2011.

UE24CS643BA1: Million Way Parallelism

With increasing amount of computation being done due to compute intensive applications like machine learning and audio/video processing, it is imperative to understand various parallel programming models. The student must also become familiar with various different hardware choices and the design choices. The course will also introduce various tools to work.

Course Objectives:

- Introduce the various parallel programming models required to scale.
- Introduce applications that benefit from scalability.
- Introduce different types of hardware such as multi-core CPUs, GPUs and FPGAs.
- Understand and use the tools to analyze FGPA Application and impact of role of various other system components on extracting performance in parallel programs.

Course Outcomes:

At the end of the course the student will be able to,

- Choose the right programming model for a problem.
- Demonstrate development of applications on different types of hardware and evaluate the choice of the right type of hardware to solve the problem.
- Demonstrate use of tools for developing parallel applications and debugging them.
- Analyze systems for issues in performance.

Course Content:

Unit 1: Introduction and Parallel Program Design: Multicore, Taxonomy, Performance Metrics, Amdahl's Law, Gustafson's law, Decomposition patterns, Program structure patterns. Matching program structure with decomposition.

14 Hours

Unit 2: Shared Memory Programming – Open MP: Threads, design concerns, semaphores, applying semaphores, debugging multithreaded applications, OpenMP- loop level parallelism, and Task level parallelism, Synchronization, Correctness and Optimization. Case Study.

14 Hours

Unit 3: GPU Programming – CUDA: GPU architecture, CUDA - programming model, execution model, Memory hierarchy. Optimization techniques, Debugging, Case Study.

14 Hours

Unit 4: FPGAs – Applications & Trends: Motivation, FPGA capabilities, Elements – Look up table, switches, logic blocks, interconnect, I/O blocks, multipliers, memory blocks, technology mapping, placement, bitstream generation. FPGA application – Machine learning , power considerations, memory systems (3D), Interconnection Networks.

14 Hours

Tools / Languages: OpenMP, CUDA.

Text Book(s):

1:"Multicore and GPU Programming: An Integrated Approach", GerassimosBarlas, Morgan Kaufmann, 2015.

Reference Book(s):

1: "Programming Massively Parallel Processors: A Hands-on Approach", David Kirk and Wen- meiHwu, Morgan Kaufmann, 1st edition, 2010.

2: "Reconfigurable Computing: The Theory and Practice of FPGA-Based Computation", Scott Hauck and Andre Dehon, Morgan Kaufmann 2008.

UE24CS643BA2 : Speech and Natural Language Processing

Speech and Natural language processing (SNLP) is one of the most important technologies of the information age. The objective of NLP is to make machines to read, decipher, understand, and make sense of the human languages in a manner that is valuable. Speech and Natural Language Processing today powers many key real- life industry applications, such as Language Translation, Dialog Systems / Chatbots, Sentiment Analysis, Text Summarizers, Speech Recognition, and Autocorrect.

Course Objectives:

- Understand the business relevance of speech and natural language technologies.
- Introduce the basic models used for processing speech and natural language.
- Work with tools to perform speech/natural language processing.
- Gain a practical insight into solving these problems.

Course Outcomes:

At the end of the course the student will be able to

- Demonstrate the use of speech/natural language processing in solving real-life problems.
- Demonstrate the use of tools for performing speech/NLP.
- Demonstrate capability to perform analysis and compare various models.
- Work in a team to solve speech/NLP related problems.

Course Content:

Unit 1 : Introduction: Business relevance, Survey of English Morphology (inflectional and derivational morphology), Finite State Morphological parsing, Porter Stemmer, Word and Sentence Tokenization, Detection and Correction of Spelling Errors, Minimum Edit Distance. **Ngrams** – Word Counting in Corpora, Simple (unsmoothed) N-Grams, Training and Test Sets, Evaluating N-Grams, Smoothing. **Vector Semantics and Embeddings -** Lexical Semantics, Vector Semantics, Words and Vectors, Cosine for measuring similarity, TF-IDF, Word2vec**.**

14 Hours.

Unit 2 : Part of Speech Tagging: English Word Classes, Tagsets for English, Part-of-Speech Tagging. **Hidden Markov and Maximum Entropy Models** – Markov Chains, Hidden Markov Model, Likelihood Computation, Decoding, HMM Training, Maximum Entropy Models. **Lexical Semantics** – Word Senses, Relation between Senses, Wordnet: Database of Lexical Relations, Event Participants, Primitive Decomposition, Metaphor, Computational Lexical Semantics.

14 Hours.

Unit 3 : Word Sense Disambiguation (WSD): Supervised Word Sense Disambiguation, WSD Evaluation, Minimally Supervised WSD, Word Similarity, Semantic: Role Labeling. **Syntactic Parsing** – Parsing as Search, Ambiguity, Search in the Face of Ambiguity, Dynamic Programming Parsing Methods, Partial Parsing, Statistical Parsing – Probabilistic CFGs, Probabilistic CKY Parsing, Ways to Learn PCFG, Rule Probabilities, Problems with PCFGs, Improving PCFGs, Probabilistic Lexicalized CFGs, Evaluating Parsers. Dependency Parsing.

14 Hours.

Unit 4 : Phonetics: Speech Sounds and Phonetic Transcription, Articulatory Phonetics, Phonological Categories and Pronunciation Variation, Acoustic Phonetics and Signals, **Automatic Speech Recognition** – Speech Recognition Architecture, HMM Applied to Speech, Feature Extraction: MFCC Vectors, Acoustic Likelihood Computation, Lexicon and Language Model, Search and Decoding, Embedded Training, Word Error Rate.

14 Hours.

Tools: Gensim, SpaCy, IBM Watson, Natural Language Toolkit (NLTK), MonkeyLearn, TextBlob, Stanford Core NLP, Google Cloud Natural Language API, …

Text Book(s):

1: “Speech and Language Processing: An Introduction to Natural Language Processing”, Daniel Jurafsky and James H. Martin, Prentice Hall, 2009.(Draft copy ,3rd Edition,2018 can be referred)

Reference Book(s) :

1: “Computational Linguistics and Speech Recognition”, Dan Jurafsky, James H. Martin, Prentice Hall, 2nd Edition, 2008.

2: “Foundations of Statistical Natural Language Processing”, Christopher D. Manning and Hinrich Schütze, MIT Press, 1999.

3: “Natural Language Understanding”,James Allen, Benjamin/Cummings publishing Company, 2ndedition, 1995.

4: “Digital Processing of Speech Signals”, Lawrence R. Rabiner, Ronald W. Schafer, Prentice Hall, 1978.

UE24CS643BA3 : Topics in Computer and Network Security

This course gives an overview and conceptual understanding of security aspects involved in a network of computers. Students will have opportunities to participate in well-designed hands-on sessions and case study discussions.

Course Objectives:

- To provide an overall view of Network Security. To understand the security problems associated in the design and implementation of the TCP, IP/ICMP, ARP protocols by analysing the network packets.
- To learn the vulnerabilities in DNS protocol and to implement and experiment with Firewall rules.
- To provide an overview of network management techniques and the usage of VPN.
- To analyse the risk management and security aspects of wireless networks.

Course Outcomes:

At the end of this course, the students will be able to:

- Sniff packets from clients and analyse them to extract important info such as headers, passwords etc.
- Launch DoS and MITM attacks using various protocol vulnerabilities and mitigate them.
- Configure firewalls on Linux machines and exploit vulnerabilities on DNS protocol. Design and implement VPN for a secure connection over internet.
- Master in wireless network security systems in depth and perform effective network management.

Course Contents:

Unit 1: Packet Sniffing & Spoofing MAC Layer and Attacks: Packet Sniffing and Spoofing: Introduction, Sending packets: Network Interface Card (NIC), BSD packet filter (BPF). Packet sniffing: Receiving packets using sockets, Packet sniffing using Raw sockets, Packet sniffing using PCAP API, Processing captured packets. Packet spoofing: Sending normal packets using sockets, Constructing spoofed raw ICMP packets and UDP packets. Sniffing and then spoofing, Python vs Scapy, Endianness. MAC layer and attacks: The MAC layer, ARP protocol, ARP cache poisoning attacks, MITM using ARP cache poisoning, Demo, Countermeasure. Network layer: IP, ICMP and attacks: IP protocol, IP fragmentation, Attacks using IP fragmentation: Problem and solution, Routing, and spoofing prevention, ICMP protocol, ICMP redirect attack, Smurf and other ICMP attacks.

14 Hours

Unit 2: TCP Attacks and DNS Attacks: Attacks on the TCP protocols: TCP overview, Send and receive buffers, SYN flood attack: TCP 3-way handshake, the SYN flooding attack, Launching the attack using Netwox and C, Countermeasure. TCP reset attack: TCP reset attack on Telnet, SSH and video streaming connections. TCP session hijacking attack: TCP session and session hijacking, launching the attack, Hijacked TCP connection. Reverse shell: working, redirecting IO to TCP connection, Creating reverse shell. Counter measure. Case Study – 1. DNS Attacks: DNS hierarchy, zones and servers, DNS query process, Constructing DNS request and response using Scapy, DNS attacks: Overview, Local DNS cache poisoning attack, Remote DNS cache poisoning attack (Kaminsky attack), Reply forgery attacks from malicious DNS servers, Countermeasure against DNS spoofing attacks,

14 Hours

Unit 3: Firewalls, IDS, IPS: Firewall: Introduction, Requirements of a firewall, Firewall characteristics and Access policy, Types of firewalls, NG firewall, Shortcomings, Firewall location and configuration: DMZ networks, Firewall topologies. Introduction, Build a simple firewall, Netfilter, iptables firewall in Linux, Stateful firewall and connection tracking, Application/Proxy firewall and Web proxy, Evading firewalls. Intrusion Detection and Prevention: Intruders, Intrusion detection, Analysis approaches, Host-based intrusion detection, Network-based intrusion detection, Distributed or hybrid intrusion detection, Honeypots, Example system: Snort, Intrusion prevention system. SOC, SIEM.

14 Hours

Unit 4: Virtual Private Network and Wireless Network Security: Case Study – 2, Virtual Private Network: Introduction, Why VPN, analogy, and tunnelling. Overview of TLS/SSL, VPN: Establishing a tunnel, Forwarding, and releasing IP packets, TLS/SSL VPN details. Building, Setup and Testing VPN. Bypassing Firewall using VPN. Wireless Security: Communications and 802.11 WLAN standards: Wired Equivalent Privacy (WEP), Wireless Protected Access (WPA), IEEE 802.1x, 802.11i/ WPA2, Wireless Network Threats.

14 hours

Note: Course includes hands-on experience on specific topics in the form of Lab and/or Assignment along with relevant cyber security case study discussions

Tools / Languages: SEED Ubuntu VM, Wireshark, Snort, Netwox, Scapy.

Text Book(s):

1: “Internet Security: A Hands-on Approach”, Wenliang Du, 3rd Edition, 2019.

Reference Book (s):

1: “Computer Security: Principles and Practice”, William Stallings and Lawrie Brown, Pearson Education, 3rd Edition, 2010.

Labs

#	Lab Task
1	Packet Sniffing & Spoofing using Scapy
2	Packet Sniffing & Spoofing using PCAP
3	ARP Cache Poisoning Attack Lab
4	ICMP Attack Lab
5	TCP Attack Lab
6	Local DNS Cache Poisoning Attack
7	Remote DNS Cache Poisoning Attack
8	Firewall Lab
9	Firewall Evasion Lab
10	VPN lab
11	Heartbleed Attack Lab (Optional)

Assignment

#	Assignment Task
1	Case Study I : iPremier
2	Case Study II : University of Virginia

UE24CS644BB1 : Advances in Cloud Computing

Cloud Computing Architecture has been revolutionizing IT development. The benefits which are achieved with Cloud environments are harnessed significantly by using development models and architectures. Cloud native architectures enable the leverage of the cloud benefits; the course will introduce Cloud Native Architectures with specific focus on microservices as the design principle.

Course Objectives:

- Introduce students to various aspects of Serverless computing.
- Introduce students to cloud native architectures and evaluate different alternatives.
- Explore and demonstrate cluster management and Infrastructure as Code (IaC) tools.
- Understand the principles of performance management and Security of Cloud Applications.

Course Outcomes:

At the end of the course,

- Students will have an ability to apply the concepts of Serverless Computing using AWS Lambda
- The students will have an ability to critically evaluate various alternatives of cloud native architectures and manage service to service communications via service mesh
- Students will be able to build and deploy cloud native applications using Dockers, Kubernetes and IaC tools such as Terraform and Ansible.
- Students will be able to apply the concepts of performance management, use tools that provide monitoring and alerting functionalities for cloud-native environments and apply security design principles in the cloud environment.

Course Content:

Unit 1: Serverless Computing: Introduction, FaaS, understanding serverless architectures, Serverless pros and cons, Serverless Framework, architectures and patterns, AWS Lambda .

14 Hours

Unit 2: Basics of Cloud Native Architecture: Fundamentals of cloud native applications, Cloud Native vs Traditional architectures, Functions vs. Services, From VMs to Cloud Native, API Design and Versioning, Service communication, Gateways, Service Mesh.

14 Hours

Unit 3: Kubernetes and Terraform: Kubernetes: Cluster architecture, Kubernetes Services, Illustration of managed Kubernetes services, working with Kubernetes Objects – deployments, Pods, scheduler, managing resources, utilities to work with resources. Terraform: Infrastructure as code, Terraform in practice, Terraform Vs. Kubernetes., Terraform Vs Ansible

14 Hours

Unit 4: Performance management and Security of cloud applications.: Application performance management in cloud environments – public, private, hybrid, IaaS, PaaS, SaaS, KPIs/metrics. User experience management - various industry and government organization standards, APM approaches - command-and-control, dynamic policy rules. Performance Monitoring tools such as Prometheus and Grafana Guiding Security design principles for Cloud Computing, Identity and access management, Single Sign-on, Identity Federation, Identity providers and service consumers.

14 Hours

Tools/Languages: AWS, Kubernetes, Terraform, Ansible, Prometheus and Grafana

Text Book(s):

1 : Cloud Native Using Containers, Functions, and Data to Build Next-Generation Applications by Boris Scholl, Trent Swanson & Peter Jausovec, O'Reilly, First Edition, 2019.

2: Application Performance Management (APM) in the Digital Enterprise - Managing Applications for Cloud, Mobile, IoT and eBusiness by Rick Sturm Carol Pollard Julie Craig, Morgan Kaufman, 2017

3. Serverless Architectures on AWS by Peter Sbarski, Yan Cui, Ajay Nair, Manning Publications, Second Edition, 2022.

Reference Book(s):

1: "Cloud Native Architectures", by Tom Laszewski , Kamal Arora , Erik Farr, Publisher Packt, 2018 2: "Cloud Native DevOps with Kubernetes" by John Arundel, Justin Domingus, O'Reilly,2019.

3: "Securing The Cloud: Cloud Computing Security Techniques and Tactics" by Vic (J.R.) Winkler, Syngress/Elsevier, 2011

4. "Terraform Up and Running, Writing Infrastructure as Code", Yevgeniy Brikman, Third Edition, O'Reilly, 2022

5. Prometheus: Up & Running, Infrastructure and Application Performance Monitoring by Brian Brazil, O'Reilly, 2018

6. Ansible for Devops, Jeff Geerling, Lean Publishing, 2020

UE24CS644BB2 : Virtual Reality & its applications

The physical entity is simulated into virtual or the imaginary environment which is designed as software or as a program that defies the beliefs of a user compelling him/her to accept it as actual reality. Virtual Reality actually exploits and plays with the sensations & perceptions of our brain by simulating an artificial environment that actually doesn't really exist, but our brains think that it does it's just like make-belief.

Course Objectives:

- Understanding basics of virtual reality through human perception.
- Introduce the use of geometric transformations on graphics objects and their application in composite form and its implementation.
- Modelling 3D world using Unity3D with the knowledge of 3D geometry.
- Exploring applications in the area of Virtual Reality using Motion sensing and Tracking.

Course Outcomes:

At the end of this course, the student will be able to:

- Demonstrate the fundamentals of human physiology in the context of virtual reality.
- Apply understanding of graphical rendering to build graphical application using OpenGL and a pply techniques of 3D geometry for building intuitive graphical applications.
- Apply techniques and tool to design an immersive virtual reality experience and use Unity3D to develop complex

  graphical applications including 3D interactive games.
- Apply graphics in greater depth to more complex courses like Image Processing, Virtual Reality, etc...

Unit 1: Introduction and Human Perception: Introduction to Virtual reality, Modern VR Experience, History, Bird's Eye View, *Hardware, software, Human Physiology and Perception, The* Human Eye, cameras, displays, Visual Perception: Perception of Depth, motion and Colour, Combining sources of information; Audio: Auditory perception auditory rendering; Frontiers; Touch and proprioception, smell and taste, robotic Interfaces, Brain Machine Interfaces.

14 Hours

Unit 2: 3D Computer Graphics: Visual rendering: Ray tracing and shading models, Rasterization, Correcting Optical Distortions, Improving Latency and framerates, Immersive Photos and videos, The OpenGL: The OpenGL API, Primitives and Attributes, Colour, Viewing, Control Functions, Polygons.

14 Hours

Unit 3: Geometric Objects and Transformations: Scalars, Points and Vectors, Three-Dimensional Primitives, Coordinate Systems and Frames, Modelling a Coloured Cube, Overview of 2D Transformations: Rotation, Translation and Scaling, Affine transformations, Transformation in Homogeneous Coordinates, Concatenation of Transformations, OpenGL Transformation Matrices, Interfaces to Three Dimensional Applications, Quaternion's.

14 Hours

Unit 4: Tracking and Intelligent VR: Motion in Real and Virtual World: Velocities and Acceleration, Physics in the virtual world, Mismatched Motion and Vection. Tracking: Tracking in 2D orientation, tracking 3D orientation, Tracking Position and Orientation, Tracking Attached Bodies, 3D scanning and Environments. Axis-Angle Representations of Rotation, Reactive AI: Adaptability, Complexity and Universality, Feasibility, More Intelligence in the System: Deliberative AI, Reinforcement learning through interaction, Imitation Learning through human demonstration.

14 Hours

Tools/Languages: C++, Unity3D, Blender

Textbook(s):

1: Virtual Reality, Steven M LavValle, University of oulu, Cambridge University press, 2020 (Available for downloading at http://lavalle.pl/vr/)

2: Creating Augmented and Virtual Realities, by Erin Pangilinan, Steve Lukas, Vasanth Mohan, PUBLISHED BY:O'Reilly Media, Inc.PUBLICATION DATE:March 2019

Reference Book(s):

1: "Interactive Computer Graphics - A top-down approach with shader-based OpenGL", Edward Angel and Dave Shreiner, Pearson Education, Sixth edition, 2012.

2: Unity Game Development in 24 Hours , Geig, Mike. Sams Teach Yourself . Pearson Education, 2014.

UE24CS644BB3: Software Security

This course will present security aspects from a secure software life cycle process – requirement, architecture, design, coding, and testing. Students will have opportunity to dwell well in to technical "how to" with hands-on sessions, assignments, and some case study discussions.

Course Objectives:

- To understand various cyber threats and attacks and secure software development process.
- To learn attack and defence mechanisms for buffer overflow, shellshock attack, etc.
- To understand the concept of threat modelling and its application.
- To learn about the most common web application security vulnerabilities and apply various penetration testing techniques and tools.

Course Outcomes:

At the end of this course, the student will be able to:

- Identify possible misuse cases in the context of software development.
- Defend against various attacks and how to write secure code.
- Apply threat modelling techniques to expose inherent vulnerabilities in applications.
- Design and develop secure web applications and exploit software vulnerabilities and launch attacks.

Desirible Knowledge : UE24CS645A – Cyber Security Essentials

Course Content:

Unit 1: Introduction and Privilege Escalation Attacks: Software Threats, Attacks and Vulnerabilities, CIA Triad, OWASP Top 10, CVE, Security and reliability, Security vs. privacy, Cyberattack Types, Anatomy of an Attack, Security Concepts and Relationships. Use cases and Misuse cases, Misuse case legend, Security use case vs Misuse case, Secure Software Development Life Cycle (SDL). Case Study: Target case study. Set-UID program: Need for privileged programs, Set-UID mechanism, Superman story, Attack surfaces, Invoking other surfaces, Principle of least privilege. Environment variables and attacks: Environment variables, Attack surface, Attacks via Dynamic linker, External program, and Library. Lab: Set-UID program & Environment variables and attacks. Shellshock attack on Set-UID and CGI programs.

14 Hours

Unit 2: Software Vulnerabilities and Malicious Software: Buffer overflow attack: Program memory layout, Stack and function invocation, Stack buffer-overflow attack, Attacks with Unknown address and Buffer size, Shellcode, Countermeasures & Defeating it. Return-to-libc attack: Introduction, Launch the attack part I & part

II. Format string vulnerability: Introduction to functions and format string, Vulnerable program, Exploiting the vulnerability, Code injection attack, Countermeasures. **Case study: Target case study**. Malware and its Types, Malware analysis: Conifer, Morris, Stuxnet worm, Ransomwares.

14 Hours

Unit 3: Threat modelling and Basic Web Security: Threat Modelling, Trust Boundaries, Attack Surfaces, Brainstorming, Modelling Methods, STRIDE model and variants, Defensive tactics, and Technologies, Privacy Threats, Taxonomy and Types. Web security basics, Attacks on HTTP GET and POST services, Cross Site Request Forgery (XSRF/CSRF): Cross-site requests and its problems, CSRF attacks, Countermeasures. **Case study: Apple - Privacy vs Safety.**

14 Hours

Unit 4: Web application security and Penetration Testing: (XSS/CSS) Attack: CSS attack, CSS attacks in action, Self-propagation, Preventing CSS attacks. SQL injection attack: Introduction to SQL, interacting with database in web, Launching SQL injection attacks, Countermeasures. Static analysis, Penetration testing: Introduction, Benefits, Drawbacks, Penetration testing tools and Fuzzing, Patching.

14 Hours

Note: Hands-on experience for relevant topics in the form of Lab and/or Assignment is given. Relevant cyber security case study for undergraduate students is discussed.

Hands-on exercises:

1. Set-UID program & Environment variables and attacks
2. Shellshock attack.
3. Buffer overflow attack
4. Return-to-libc attack.
5. Format string vulnerability.
6. CSS/XSS attack
7. CSRF attack.
8. SQL injection.
9. Penetration testing.(Assignment)
10. Malware 1,2,3 (Assignment)
11. Case study 1,2 (Target, Apple)

Tools / Languages: SEED Labs VM, Scapy, Burp Suite, Metasploit, Nmap, etc.

Text Book(s):

1: “Computer & Internet Security: A Hands-on Approach”, Wenliang Du, 2nd Edition/3rd Edition.

Reference Book(s):

1: “Computer Security: Principles and Practice”, William Stallings and Lawrie Brown, Pearson Education, 3rd Edition, 2014.

2: “Secure Programming with Static Analysis”, Brian Chess and Jacob West, Pearson Education, 2007

UE24CS645BC1 : Advanced Big Data Analytics

The course explores the big data analytics lifecycle: question formulation, data collection and cleaning, exploratory analysis, statistical inference, prediction and decision-making. Focuses on building analytical models using key principles and techniques.

Course Objectives:

- Introduce alternative techniques to perform big data processing.
- Introduce applications of Big Data Processing.
- Use tools and techniques to analyze streaming data
- Introduce Technologies for performing text/Sentiment/Video/Image analysis

Course Outcomes:

At the end of the course the student will be able to

- Motivate and explain trade-offs in big data processing technique design and analysis in written and oral form.
- Demonstrate the usage of Spark to handle big data workloads.
- Demonstrate development of analytics applications using GCP and Azure.
- Demonstrate ability to do text, video, Image analysis of an application using NLP

Course Content:

Unit 1: Introduction and MapReduce: Introduction, HDFS overview, formats, MapReduce architecture, YARN, limitations of MapReduce, Algorithms: PageRank, Alternatives to Map Reduce – Iterative, Workflow processing, Workflow model case study.

14 Hours

Unit 2: In Memory processing: Graph Processing, In-memory computation., Apache Spark – RDDs, Scala Performance advantages, Introduction to machine learning. Machine learning with Spark.Clustering, and Collaborative filtering Algorithms applied to Big Data.

14 Hours

Unit 3: Streaming analytics: Overview, Optimize streaming analytics and use cases, Building stream pipelines on Azure, Streaming Analytics with Azure Databricks, Sizing considerations for Stream Analytics deployments, A Training course on Stream processing, Algorithms for pattern matching, aggregations, filtering and time correlations using Spark Streaming

14 Hours

Unit 4: Text, Video, Image Analytics: Text analytics, Text mining, Video Analytics, Image Analytics and Natural Language Processing

14 Hours

tools/Languages: Apache Hadoop, Spark, R/Python

Text Book(s):

1: “Big Data Analytics Beyond Hadoop”: Real-Time Applications with Storm, Spark, and More Hadoop Alternatives,Vijay Srinivasa Agneeswaran PhD, 1st Edition, Pearson, 2014.

Reference Book(s):

1: “Mining of Massive Datasets”, AnandRajaraman, JureLeskovec, Jerey D. Ullman, 2nd Edition, Cambridge University Press, 2014.

2: Abu-El-Haija, Sami, Nisarg Kothari, Joonseok Lee, Paul Natsev, George Toderici, Balakrishnan Varadarajan, and SudheendraVijayanarasimhan. "Youtube-8m: A large-scale video classification benchmark."arXiv preprint arXiv:1609.08675(2016).

3: Huang, Qi, PetcheanAng, Peter Knowles, Tomasz Nykiel, IaroslavTverdokhlib, Amit Yajurvedi, Paul Dapolito IV et al. "SVE: Distributed video processing at Facebook scale." In Proceedings of the 26th Symposium on Operating Systems Principles, pp. 87-103.ACM, 2017.

UE24CS645BC2 : Deep Learning Theory and Practices

Deep Learning has received a lot of attention over the past few years and has been employed successfully by companies like Google, Microsoft, IBM, Facebook, Twitter etc. to solve a wide range of problems in Computer Vision and Natural Language Processing. In this course we will learn about the building blocks used in these Deep Learning based solutions. At the end of this course students would have knowledge of deep architectures used for solving various Vision and NLP tasks.

Course Objectives:

- To impart knowledge on Feed Forward Neural Networks.
- Introduce students to Convolutional Neural Networks and Transfer Learning.
- Provide in-depth coverage of Sequence Modelling.
- Introduce students to Auto encoders. Generative Adversarial Networks and Graph Neural Networks.

Course Outcomes:

At the end of this course, the student will be able to:

- Develop a simple Feed Forward Neural Network using Multilayer Perception.
- Classify images using CNN.
- Solve time-series related problems with RNN.
- Use efficient data representations using Auto encoders and generate data in the form of images using Generative AI models.

Course Contents

Unit 1: Introduction to Deep Learning: CNN Model & Transfer Learning: Introduction**,** Activation functions, Loss functions, Batch Normalization, Regularization and Optimization. **Convolutional Neural Network(CNN):** Introduction, Filters, FeatureMaps, Max-Pool Layers, Other Pooling Types, Back Propogation. Convolution Architectures - Alexnet, ZFNet, VGGNet, GoogleNet, ResNet. **Transfer Learning**: Introduction, Motivation, Variations, TL Architecture of CNNs.Hands-on: Assignment on CNN & TL.

14 Hours

Unit 2: Recurrent Neural Networks (RNN): Introduction-Recurrent Neurons, Memory Cells, Variable-Length Input-Output Sequences, RNN Architecture, Sequence learning problem, BPTT-Back Propagation Through Time, truncated BPTT, Vanishing and Exploding Gradient, Bidirectional RNN, LSTM Cell and GRU Cell, Text Classification with RNN, Encoder/Decoder architecture, Seq2Seq model with Attention, Transformer model and BERT architecture, Transformer Attention.

14 Hours

Unit 3: Generative Models and GNNs : Introduction to Autoencoders , Regularization in autoencoders, Denoising autoencoders, Sparse autoencoders, Contrastive autoencoders , Variational Auto Encoders(VAEs). **Generative Adversarial Networks**(GANs)- Architecture and Training Methods, Image Generation, DCGAN, Style GAN, WGAN, Applications.**Graphical Neural Networks(GNN)**: Introduction to GNNs, Graph Convolution Networks, Applications.

14 Hours

Unit 4: Reinforcement Learning, **Diffusion Models, Federated Learning and Overview of Latest Deep Learning Models:** Introduction, Basic Framework of RL, Learning to Optimize Rewards, Credit Assignment Problem, Temporal Difference, Learning and Q Learning. **Deep RL:** Deep Q Learning, Training and Testing. **Diffusion Model**, Stable diffusion architectures, Introduction to Vision Transformers, GPT Architecture. **Federated Learning:** Horizantal, Vertical and FTL (Federated Transfer Learning).

14 Hours

Tools/ Languages: Pytorch.

Text Book(s):

1: “Advanced Deep Learning with Python” - Ivan Vasilev, Packt Publishing, 2019.

2: “Neural Network and Deep learning” by Charu C Agarwal. Springer International Publishing 2018. Book)

3: “Deep Learning”, Ian Goodfellow, YoshuaBengio, Aaron Courville http://www.deeplearningbook.org/ (E-Book)

Reference Book(s):

1: “Hands-on Machine Learning with Scikit-Learn and TensorFlow”, Aurelian Geron, O’REILLY, 1st Edition, 2017. 2: “Deep Learning with Keras”, Antonio Gulli and Sujit Pal, Packt Publishing, 1st Edition, 2017.

3: “Pattern Recognition and Machine Learning”, Christopher Bishop, Springer, 1st Edition, 2011 (Reprint).
4:Handouts: Transfer Learning / Latest Deep Learning Techniques / Vision Transformers/ GPT / FL

UE24CS645BC3: Cryptography

Cryptography is the science of securing data by using mathematical concepts. Cryptography involves the authentication and verification of data in all domains by applying Cryptographic protocols.

Course Objectives:

- Enable to learn the fundamental concepts of cryptography and utilize these techniques in computing systems.
- Discuss various encryption techniques and mathematics behind them..
- Understand the concept of public key Cryptography and message authentication and hash function.
- Understanding different attacks to help gain deeper insight into Cryptography.

Course Outcomes:

At the end of the course the student will be able to,

- Appreciate the impact of cyber-attacks on society and the necessity of cryptography.
- Analyse Cryptographic techniques using the mathematical foundations of cryptography.
- Design applications/protocols using cryptographic techniques.
- Apply cryptanalysis to solve real time problems and Evaluate the authentication and Hash Algorithms.

Course Content:

Unit 1: I**ntroduction to Cryptography:**Why Cryptography? Security trends – legal, ethical and professional aspects of security, Basic Cryptographic primitives (encryption, decryption, signatures, authentication), Classical encryption techniques : substitution technique, transposition techniques, Steganography, Historical Ciphers and their cryptanalysis, Modern Cryptography: Principles of Modern cryptography, Perfectly-secret encryption – Vernam's One-time-pad encryption – Limitations, Shannon's theorem, Stream Ciphers, Block cipher design principles, Block Vs Stream cipher. Classical vs. Modern cryptography. Lab : Crypto by hand.

14 Hours

Unit 2 : Math for Cryptography: Mathematical Modular arithmetic-Euclid's algorithm, Primes, Factorization, Chinese Remainder Theorem, Algebraic structures: Groups, Rings, Fields- Finite fields **Semantic Security :** Definition of semantic security, One- Way Functions, Hardness Amplification, One-way Permutations, Trapdoor Permutations, Computational Indistinguishability, Pseudo-randomness. **Private Key Cryptography:** Private/Symmetric Key Ciphers: Fiestel network, DES, AES, Cryptanalysis: Block cipher mode of operation, Chosen-Ciphertext Attacks, Differential and linear cryptanalysis.

14 Hours

Unit 3: Key Management and the Public Key Revolution: Key distribution and Key Management, Diffie Hellman Protocol - Variations of Diffie Hellman., Challenges of Key Management in Symmetric Key Cryptography. **Public Key Cryptography:** RSA Encryption Algorithm, Implementation issues and Pitfalls, Elgamal encryption, Elliptical Curve Cryptography. **Authentication :**Message Authentication Code (MAC) – Definition, Message Integrity, Cipher Block Chaining (CBC-MAC), Constructing Secure message Authentication codes, Authenticated Encryption, Hash Functions and Applications: MAC using Hash functions HMAC. **Digital Signatures:** DSA, RSA Digital Signatures, ECDSA.

14 Hours

Unit 4 : Attacks on Cryptographic Implementations: Sophisticated attacks on block ciphers, Attacks on the anonymous Diffie-Hellman protocol, Bleichenbacher's attack on the RSA-PKCS1 encryption scheme.Case study: 802.11b WEP - a badly broken system **Zero Knowledge Proofs:** A Knowledge-Based Notion of Secure Encryption, Zero-Knowledge Interactions, Interactive Protocols, Interactive Proofs, Zero-Knowledge Proofs, Proof of knowledge, Applications of Zero- knowledge **Post Quantum Cryptographic Techniques:** Need for Post Quantum Cryptography, Introduction to Lattice Based Cryptography, Types of Lattice Based Cryptography, Hard Problems on Lattices, LWE Problem.

14 Hours

Tools / Languages: Seed virtual machine environment.

Text Book(s):

1: "Introduction to Modern Cryptography", Jonathan Katz, Yehuda Lindell, CRC Press, 2018.

2. " A graduate Course on Cryptography" Dan Boneh and Victor Shoup, Version 2023.

UE21CS841A : COMPUTER VISION

Course Objectives:

- Through this course, students are expected to
- To achieve a basic understanding of Computer Vision
- To understand Image processing and Feature detection
- To evaluate Motion Estimation and Video rendering techniques
- To analyse image recognition models.

Course outcomes:

The students should be able to

- Implement basic Image processing techniques.
- Develop feature detector and motion detector in videos.
- Model object recognition for videos

Course contents

Introduction to Computer Vision, Image Formation and Processing What is Computer Vision? Geometric primitives and transformations: 2D transformation,3D transformation; Image Processing:- Point operators: Pixel transform, Colour transforms, Compositing and matting Histogram equalization; Linear filtering: Separable filtering, Band-pass and steerable filters; More neighbourhood operators: Median filtering, Bilateral filtering, Fourier transforms; Pyramids: Interpolation, Decimation, Multi-resolution representations; Geometric transformations: Parametric transformations, Mesh-based warping, Application: Feature-based morphing **12 Hours**

Feature Detection Feature detectors: Forstner Harris, Adaptive non-maximal suppression, measuring

repeatability, Scale invariance, Rotational invariance and orientation estimation, Affine invariance, Feature descriptors: Bias and gain normalization, Scale invariant feature transform, PCA-SIFT, Gradient location-orientation histogram (GLOH) **12 Hours**

Motion Estimation 65 Translational alignment: Robust error metrics, Spatially varying weights, Bias and

gain, Correlation, Hierarchical motion estimation: Fourier-based alignment, Windowed correlation, Phase correlation Rotations and scale. Parametric motion: Patch-based approximation, Compositional approach. Learned motion models, Spline-based motion, Optical flow, Multi-frame motion estimation, Layered motion **12 Hours**

Image and Video Rendering Image matting and compositing: Natural image matting, Optimization-based matting, Smoke, shadow, and flash matting, Video matting; Texture analysis and synthesis: Application:

Hole filling and inpainting, Application: Non-photorealistic rendering, Neural style transfer and semantic image synthesis Video textures, 3D Video, Neural Rendering

10 Hours

Recognition and Video Compression: Object detection: Fast RCNN, Faster RCNN, Semantic segmentation: U Net, Triamasu Model; Pose estimation, Video understanding. Video coding, representation -Vide Standards: MPEG 1, 2, MPEG-4, H.261, H.263, H.264. Video compression - Interframe Compression - 3D Waveform based – Motion Compensation

10 Hours

Textbook

1. Computer Vision: Algorithms and Applications", Richard Szeliski, 2021

https://www.dropbox.com/s/vdohbj8i4xq838s/SzeliskiBookDraft_20210214.pd

f?dl=0

2. Computer Vision: Algorithms and Applications", Richard Szeliski, 2nd

Edition, Springer, 2010.

3. The Essential Guide to video processing-Al Bovik (Alan C Bovik), Academic

Press,2009

UE21CS842A: Data Mining

Unit I-

Introduction, Getting to know your Data and Data Preprocessing: Data Mining Process, Data Mining - CRISP DM approach, Data Mining Applications, Data Mining Techniques, Practical examples of data mining, Future of Data Mining, Guidelines for successful data mining, Data collection and pre-processing, Outliers, Mining outliers, Missing data, Types of data, Computing distance, Data summarising: Using basic statistical measurements.

Unit II-

Mining Frequent Patterns, Association and Correlations: The task and the naïve algorithm, Apriori algorithm, improving efficiency of the Apriori algorithm, Apriori - TID, Direct hashing and pruning DHP, Dynamic Itemset Counting DIC, Mining frequent patterns without candidate generation, performance evaluation of algorithms.

UNIT III-

Classification: Decision tree, building a decision tree, split algorithm based on information theory, split algorithm based in Gini Index, Overfitting and Pruning, Decision tree rules, Naive Bayes method, estimating predictive accuracy of classification methods, Improving accuracy of classification methods, other evaluation criteria, Classification software (Chapter 3 and 4) (Book 1).

Unit IV-

Cluster analysis: Desired features, Cluster analysis methods, Partitional methods, Hierarchical methods, Density based models, Dealing with large database, Quality and validity of cluster analysis methods, Cluster analysis software.

Unit V-

Data Warehousing and OLAP: Data warehousing basic concepts, Data warehousing models: Data Cube and OLAP, Data Warehouse Design and Usage, Datawarehouse Implementation, Data generalization by attribute-oriented induction. 69

Reference Books: 1.Data mining with Case Studies, G K Gupta, 3rd edition, 2014,PHI. 2.Data Mining concepts and Techniques Authors: Jiawei Han, Micheline Kamber, Jian Pei. 3rd edition, 2011, Elsevier/Morgan Kaufmann.

UE21CS843A: Natural Language Processing

The goal of this course is to focus on processing of text data as found in natural language usage. The key problem discussed in this course is that of understanding the meaning of text by various types of learning models including the recent approaches using deep learning and the significance of the NLP pipeline in that meaning disambiguation process. The course also discusses disambiguation of syntax as a step of meaning disambiguation process. This course requires the student to have a desirable knowledge of Machine Intelligence.

- **Course Objectives:**
- Learn the central themes, learning problem and the problem solving approaches used in NLP.
- Focus on various learning models related to sequence labelling that is the basic building block in NLP.
- Learn how syntactic disambiguation is done in NLP.
- Learn how lexical and distributional semantics can be used for semantic disambiguation in NLP.
- Introduce the deep learning techniques and its applications in Natural Language Processing.

Course Outcomes:

At the end of this course, the student will be able to:

- Have a very clear understanding of the central themes, central problem being solved in NLP and the learning approaches used in solving them.
- Get a grip on various sequence labelling approaches and applications in NLP.
- Get a grip on how syntactic ambiguity removal can contribute in overall disambiguation process.
- Apply comfortably & confidently to the appropriate branch of semantics depending on the problem being solved.
- Learn how to implement neural language model, NLP applications using neural techniques and utilize various transfer learning approaches in NLP.

Desirable Knowledge: UE19CS303-Machine Intelligence.

Course Content:

Unit 1: Introduction: Introduction, Knowledge in Language Processing, Types of ambiguity in natural language processing, Models and Algorithms,**Text normalization:**Content and Function words, type vs. token, word tokenization and normalization, Morphological parsing of words – Porter stemmer,

Lemmatization and Stemming, Sentence segmentation. **Noisy Channel model:** Real world spelling error, Minimum edit distance algorithm, Concept of noisy Channel Model. **10 hours**

Unit 2: Language Models and Semantics(Lexical and Vector): N-grams,n-gram language model, smoothing, discounting and back-off, Kneser-Ney smoothing, interpolation, perplexity as an evaluation measureWord senses and relations between word senses, WordNet: A Database of Lexical Relations; Word sense disambiguation : supervised word sense disambiguation, WSD : dictionary and thesaurus methods, semi-supervised WSD, unsupervised word sense induction Semantic relatedness based on thesaurus like WordNet : Resnik similarity, Lin similarity, Jiang-Conrath distance, Extended Gloss overlap and Extended Lesk method. Lexicons for sentiment and affect extraction: available sentiment and emotion lexicons. Vector Semantics and Embeddings: Words and vectors, TF IDF, Pointwise Mutual Information, Measuring similarity, Using syntax to define a word's context, Evaluating vector models, Dense vectors via SVD Distributional Hypothesis, Neural Embedding: skip gram and CBOW Pre-trained word representations: Word2Vec and Glove, Improving Word2vec: FastText, Limitation of distributional methods. - **12 Hours**

Unit 3: Handling sequences of text: Sequence labelling: Sequence labelling as classification, sequence labelling as structure prediction, Viterbi algorithm and Hidden Markov Model, POS Tagging example, POS Tagging using discriminative models i.e. Maximum Entropy Markov Model (MEMM). Discriminative Sequence labelling with features-Conditional Random Field. Other sequence labelling applications – Named Entity Recognition: practical NER architectures.- **12 Hours**

Unit 4: Parsing - Disambiguating Structure : Constituency parsing: Ambiguity presented by parse trees, CKY parsing,Span-based Neural Constituency Parsing, CCG Parsing, Partial parsing – chunking. **Statistical Parsing :** Probabilistic Context Free Grammar, Probabilistic CKY parsing of PCFG, Problems with PCFG, Probabilistic Lexicalized CFG **Introduction to dependency parsing:** Dependency relations, Dependency Formalisms, Dependency Tree Banks. Evaluating parsers.**Coreference resolution:** Forms of referring expression, algorithms for coreference resolution – mention pair and mention ranking model, mention detection, classifiers using hand-built features.-

10 Hours

Unit 5: Natural Language Generation and Neural Network Methods : Neural Sequence labelling - Recurrent Neural network language model for POS tagging. **Convolutional Neural Network for text:** word level and character level language model with CNN and Sentiment analysis. **Machine Translation & Encoder -Decoder Models**: Language Divergences & Typology, The Encoder-Decoder Model, Encoder-decoder with RNNs, Attention, Beam Search, Encoder-decoder with transformers, some practical details on building MT systems, MT Evaluation, Bias & Ethical Issues. **Transfer learning in modern NLP -** BERT, ELMo, GPT, ULMfit. –

12 Hours

Tools / Languages : Tensorflow, SCIKIT Learn, Python 3.x.

CoreNLP, Natural Language Toolkit (NLTK), TextBlob,Gensim, SpaCy,PyTorch-NLP , OpenNLP.

Text Book:

1.“Speech and Natural Language Processing”, Daniel Jurafsky and James H. Martin, 2nd edition paperback,2013. The more up to date 3rd edition draft is available at http://web.stanford.edu/~jurafsky/slp3/.

Reference Book(s):

1. “Introduction to Natural Language Processing”, Jacob Eisenstein, MIT Press, Adaptive computation and Machine Learning series, 18th October, 2019.

2. **The open source softcopy is available at githubhttps://github.com/jacobeisenstein/gt-nlp class/blob/master/notes/eisenstein-nlp-notes.pdf**

UE21CS844A: IoT ARCHITECTURE AND PROTOCOLS

Course Objectives:

- To Understand the Architectural Overview of IoT.
- To Understand the IoT Reference Architecture and Real World Design Constraints.
- To Understand the various IoT Protocols (Datalink, Network, Transport, Session,
- Service).

Course Outcomes:

UNIT I Overview : What is IOT? Trends in adoption of IOT, Convergence of IT and IOT, Challenges in IoT. IoT-An Architectural Overview– Building an architecture, Main design principles and needed capabilities, An IoT architecture outline, standards considerations. M2M and IoT Technology Fundamentals- Devices and gateways, Local and wide area networking, Data management, Business processes in IoT.

UNIT II Reference architecture :

IoT Architecture-State of the Art – Introduction, State of the art, Reference Model and architecture, IoT reference Model - IoT Reference Architecture- Introduction, Functional View, Information View, Deployment and Operational View, Other Relevant architectural views. Real-World Design Constraints- Introduction, Technical Design constraints-hardware is popular again, Data representation and visualization, Interaction and remote control.

UNIT III IoT data link layer & network layer protocols : PHY/MAC Layer(3GPP MTC, IEEE 802.11, IEEE 802.15), Wireless HART,Z-Wave, Bluetooth Low Energy, Zigbee Smart Energy, DASH7 - Network Layer-IPv4, IPv6, 6LoWPAN, 6TiSCH,ND, DHCP, ICMP, RPL, CORPL, CARP 67

UNIT IV Transport & session layer protocols: Transport Layer (TCP, MPTCP, UDP, DCCP, SCTP)-(TLS, DTLS) – Session Layer-HTTP, CoAP, XMPP, AMQP, MQTT.

UNIT V Service layer protocols & security

Service Layer -oneM2M, ETSI M2M, OMA, BBF – Security in IoT Protocols – MAC 802.15.4 , 6LoWPAN, RPL, Application Layer

Textbook (s)

1. Jan Holler, Vlasios Tsiatsis, Catherine Mulligan, Stefan Avesand, Stamatis Karnouskos, David Boyle, “From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence”, 1st Edition, Academic Press, 2014.

2. David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, Jerome Henry,"IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things”, 1st Edition, Pearson Education (Cisco Press Indian Reprint). (ISBN: 978-9386873743)

3. Peter Waher, “Learning Internet of Things”, PACKT publishing, BIRMINGHAM – MUMBAI

4. Bernd Scholz-Reiter, Florian Michahelles, “Architecting the Internet of Things”, ISBN 978-3-642-19156-5

e-ISBN 978-3-642-19157-2, Springer

5. Daniel Minoli, “Building the Internet of Things with IPv6 and MIPv6: The Evolving World of M2M Communications”, ISBN: 978-1-118-47347-4, Willy Publications

6. Vijay Madisetti and ArshdeepBahga, “Internet of Things (A Hands-on- Approach)”, 1st Edition, VPT, 2014.

1. **7. http://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_p**

UE21CS845A: Fundamentals of IOT and Cryptographic Security

Unit 1- Introduction to IoT and Reference Model- Defining the IoT- Cybersecurityversus IoT security and cyber physical systems, Applications of IoT, IoT Reference model by Cisco, A Simplified IoT Architecture, The Core IoT Functional Stack, IoT Data Management and Compute stack, Smart Objects: The "Things" in IoT. **Access Technologies:** IEEE 802.15.4, LoRaWAN.

12 hours

Unit 2- IoT protocols : Optimizing IP for IoT: From 6LoWPAN to 6Lo, Routing overLow Power and Lossy Networks, The Transport Layer, Messaging protocols- Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol (COAP), Extensible Message and Presence Protocol (XMPP), Advanced Message queuingProtocol (AMQP), Representation State Transfer(REST).

12 hours

Unit 3- IoT Security- Primer on threats, vulnerability, and risks , Primer on attacks and countermeasures- Common IoT attack types, Attack Trees, Example anatomy of a deadly cyber-physical attack, Today's IoT attacks, Attacks against enterprise, Threat modeling an IoT system. **Hardware Security Risks** - Hardcoded/Default Passwords -Resource Constrained Computations -Legacy Assets Connections - Devices Physical Security, **Software Security Risks** -Software Vulnerabilities -Data Interception - Identification of Endpoints -Tamper Detection, Lack of Industrial Standards

12 hours

Unit 4- Cryptographic Fundamentals for IoT Security: Cryptography and its role insecuring the IoT, Types and uses of the cryptographic primitives in the IoT, Module principles, Key management fundamentals, Cryptographic controls built into IoTmessaging protocols and communication protocols.

10 hours

Unit 5- Attacks on Layers: Classification of Attacks on IoT: Types of attacks- Physicalattacks, Side channel attacks, Cryptanalysis attacks, Software attacks, Network attacks,Layered classification of attacks on the WSN, Layered classification of attacks on the RFID. **Attacks and Threats in IoT system model -** Attacks in Physical/Perception Layer, Attacks in Network & Transport Layer, Attacks in Application Layer.

10 hours

TEXTBOOK

1. David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Rob Barton and Jerome Henry, —IoT Fundamentals: Networking Technologies, Protocols and Use Cases for Internet of Things, Cisco Press, 2017
2. Brian Russell, Drew Van Duren -Practical Internet of Things Security
3. Mikhail Gloukhovtsev -IOT SECURITY: CHALLENGES, SOLUTIONS & FUTURE PROSPECTS

REFERENCES

1. Otmane El Mouaatamid, Mohammed Lahmer- Layered classification of Attacks and possible countermeasures
2. Debabrata Singh, Pushparaj, Manish Kumar Mishra - Security Issues InDifferent Layers Of IoT And Their Possible Mitigation

UE22CS841A : GEOMATICS ENGINEERING

1. **Geographical Concepts -1** (Pg 1-60 & 157-175)

1.1 Introduction, Geographical Concepts, GIS & Geography, Difference between image processing systems, Utility of GIS. (8 hours)

1.2 GIS Software's, Applications, Representative application areas & their foundations (3 hours)

2. **Geographical Concepts -2** (Pg 63-126)

2.1 Principles: Representing geography - Rasters & Vectors, Nature of geographic data (8 hours)

2.2 Georeferencing, Linear referencing system, measuring earth, Projections & Coordinates (3 hours)

3. **Creating & maintaining geographic data** (Pg 217-239 & Pg 315-382)

3.1 Geographic Modelling, Geovisualization, Creating & maintaining geographic data. (4 hours)

3.2 Query measurement & transformations, Descriptive summary, design and inference, spatial modelling with GIS (9 hours)

4. **Image Acquisition & Pre-processing** (Pg 61- 153 & 305-331 Book2)

4.1 Image Acquisition: Mapping Cameras, Digital Imagery, Image Interpretation (9 hours)

4.2 Pre-processing: Introduction, Radiometric processing, Image data Processing standards (4 hours)

5. **Applications of Remote Sensing (Land Use Land Cover & Plant Science)** (Pg 465-508, 585-608) 71

5.1 Introduction, Land use land cover — definition and its significance in engineering projects, History of land use land cover, Land cover classification systems, Land use land cover analysis. Visual image interpretation techniques for land use cover map preparation. (7 hours)

5.2 Plant Science: Introduction, Agriculture, Vegetative Indices, Applications of Vegetative Indices. (3 hours)

Books

1. "Geographic Information systems and science", Paul A Longley,

Michael F Goodchild, David J Maguire, David W Rhind

https://www.google.co.in/books/edition/Geographic_Information_Systems

_and_S cien/toobg6OwFPEC?hl=en&gbpv=1

2. "Introduction to Remote Sensing", James B, Campbell Randolph H,

Wynne, Guilford Press.

Introduction_to_Remote_Sensing_www.GISman.ir (1).pdf

3. "Remote Sensing and Image Interpretation", Lillesand T M and R W Kiefer, 4th Ed John Wiley.

UE22CS842A : IOT FOR CONNECTED HEALTHCARE I

The Course will introduce the role of connected health applications, such as the Internet of Things (IoT), remote care, and disease and lifestyle management in facilitating more efficient and effective care and supporting the shift from hospital to community-based care. Connected Health and the Internet of Things will focus on exploring the variety of connected health technologies and solutions currently in use or emerging in the healthcare industry. They will provide you with the best practices for their successful adoption, integration,

deployment, monitoring in clinical settings and the unique operational and privacy and security implications of these technologies.

Course Objectives:

• To learn how to design and implement IoMT applications that manages big data, streaming data, and/or distributed data.

• Equip participants with the knowledge and tools required to develop and execute strategies for adoption and integration of connected technologies in their own healthcare organizations.

• Enable participants to develop, measure, and monitor Key Performance Indicators related to the safe and effective use of connected health technologies.

• Apply best practices to ensure the security, privacy, and ethical use of connected health devices and data within regulated healthcare environments.

• To expose more about connected healthcare technologies, use cases and applications.

Course Outcomes: 57

• Connected healthcare technologies, use cases, and benefits.

• Virtual and physical infrastructure models and requirements for supporting connected health solutions.

• Best practices related to measuring and monitoring the performance of connected health solutions in clinical practice. Security and privacy best practices related to the introduction and integration of connected health solutions into healthcare organizations.

• Legal and ethical considerations related to the use of connected health devices and data in healthcare.

UNIT1-Introduction to IoT & IoMT, IoMT is important for Healthcare, How IoMT is changing medicine, Benefits, challenges and opportunities, **IoMT:** Foundation and Characterization-IoMT and Robotics, Integration of Bio-interfaces, Devices and Sensors, Remote Health monitoring

10hrs

UNIT 2: Wearable Technologies a& IoMT Fundamentals of Wearable Technologies, Wearable Chemical and Biochemical Sensors. Technology of Connected Devices – Device Types, Sensors, Actuators. Internet of Things – Devices, Objects, Physical Activity Modeling and Behavior Change. Internet of Things – Interface and Interaction Design, Human Body Communication for a Data Rate Sensor Network. Internet of Things – Networking, Wearable Sensors for Monitoring of Physical and Physiological Changes and for Early Detection of Diseases.

12hrs

UNIT 3: Data Analytics and Supporting Services: Structured Vs. Unstructured Data and Data in Motion Vs. Data in Rest, Role of Machine Learning-No SQL Databases, Hadoop Ecosystem, Apache Kafka, Apache Spark, Edge Streaming Analytics and Network Analytics, Xively Cloud for IoT, Python Web Application Framework, Django, AWS for IoT.

10hrs

UNIT 4: Human Motion Analysis Introduction**,Human motion representations and direct kinematics:** kinematic tree,3D locations,joint angles,axis angles,quaternions , **Models of Human Pose and Motion:** Latent variable models: PCA, FA, GPLVM, **Dynamical systems**: LDS, **Human motion synthesis:** ML approaches: NN (motion graphs), Inverse kinematics, LVMs,Space-time constraints: physics. **Pose estimation from images:** Inverse kinematics, **Discriminative models**: regression **Generative models:** Kalmann filters, particle filters, Likelihood models, **Human motion classification:**Gait analysis,Discriminative LVMs,Structuredoutput

methods.

10hrs

UNIT5: Security &Applications Security Requirements in IoT Architecture - Security in Enabling Technologies -

Security Concerns in IoT Applications. Security Architecture in the Internet of Things - Security Requirements in IoT - Insufficient Authentication/Authorization – Insecure Access Control - Threats to Access Control, Privacy, and Availability - Attacks Specific to IoT. **Applications:** Industrial IoT - Case Study: Healthcare (Screen Cloud, Screen metrix), Activity Monitoring.

12 hrs

Text Books:

1. David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Rob Barton and Jerome Henry, IoT Fundamentals:Networking Technologies, Protocols and Use Cases for Internet of Things, Cisco Press, 2017.

2. Edward Sazonov, Michael R. Neuman (editors), Wearable Sensors: Fundamentals,Implementation and Applications, 2014, Academic Press/Elsevier, ISBN 978-0124186620

3. Honbo Zhou, Internet of Things in the Cloud – A Middleware Perspective, 2012, CRC Press, ISBN 978-1439892992 .

4. Russell, Brian, and Drew Van Duren. Practical Internet of Things Security: Design a security framework for an Internet connected ecosystem. Packt Publishing Ltd, 2018.

Reference Books:

1. Li, Shancang, and Li Da Xu. Securing the internet of things. Syngress, 2017.

2. Hu, Fei. Security and privacy in Internet of things (IoTs): Models, Algorithms, and Implementations. CRC Press, 2016.

3. Jan Holler, Vlasios Tsiatsis, Catherine Mulligan, Stamatis, Karnouskos, Stefan Avesand, DavidBoyle, From Machine-to-Machine to the Internet of Things – Introduction to a New Age of Intelligence, Elsevier, 2014.

4. Claire Rowland, Elizabeth Goodman, Martin Chalier, Ann Light, Alfred Lui, Designing Connected Products:

UX for the Consumer Internet of Things, 2015, 60 O'Reilly Media,Inc, ISBN 978-1449372569

Sources: Connected Health and IoT (CH - IoT) – NIHI Human Motion Analysis , Spring 2010 (toronto.edu)

https://iiitranchi.ac.in/docs/syllabi/syllabus_mtech_ece.pdf Syllabus

UE23CS841A : Health Digital Twin and extended Reality

This course is an in-depth exploration of the concepts, technologies, and applications of Digital Twin and Extended Reality. Through a combination of theoretical lectures and practical projects, students will gain the knowledge and skills needed to develop intelligent systems, analyse security threats, and apply Digital Twin and Extended Reality solutions to various industries.

Course Objectives:

- Understand the fundamental concepts and technologies of Digital Twin and Extended Reality, including AR and VR, 3D transformation, AI/ML, and data visualization.
- Develop the skills needed to design and implement Digital Twin and Extended Reality solutions, including the ability to create mock, functional, and executable twins.
- Analyse security threats to Digital Twin and Extended Reality systems and apply trust modelling techniques to ensure the security and integrity of these systems.
- Apply Digital Twin and Extended Reality solutions to various industries, including industrial IoT, critical infrastructure, Agri infrastructure, and connected vehicles.
- Collaborate with peers on practical projects to gain hands-on experience in developing intelligent systems and applying Digital Twin and Extended Reality solutions to real-world problems.

Course Outcomes:

At the end of this course, the student will be able to:

- Students will be able to demonstrate a deep understanding of the fundamental concepts and technologies of Digital Twin and Extended Reality, including AR and VR, 3D transformation, AI/ML, and data visualization.
- Students will be able to design and implement Digital Twin and Extended Reality solutions, including the ability to create mock, functional, and executable twins, and apply generative AR techniques.
- Students will be able to analyse security threats to Digital Twin and Extended Reality systems and apply trust modelling techniques to ensure the security and integrity of these systems.
- Students will be able to apply Digital Twin and Extended Reality solutions to various industries, including industrial IoT, critical infrastructure, Agri infrastructure, and connected vehicles, and assess the benefits and limitations of these solutions.
- Students will be able to collaborate effectively with peers on practical projects and demonstrate the ability to apply Digital Twin and Extended Reality solutions to real-world problems, such as improving operational efficiency, enhancing safety, and reducing costs.

Pre-Requisite: UE18CS202- Data Structures.

Course Content:

Unit 1: Introduction to AR and VR: Overview of AR and VR technologies, Introduction to the OpenGL graphics pipeline, Rotation, Translation and Scaling , 3D transformation, homogeneous transformations, First OpenGL program, Controls and Animations, Vector Space, Affine Space and Euclidian Space, Affine Transformation, Transformation in Homogeneous Coordinates, 3D transformation, Homogeneous Transformations,

Concatenation of Transformation, Transformation Matrices, Interface to Three dimensional Applications, Quaternions Basics, Quaternions, multiplication and Rotation, Quaternion Visualization

14 Hours

Unit 2: Digital Twin Essentials: The Big Picture of Digital Twins, History of the Digital Twin, Origin of the Digital Twin concept, Digital Twin and Product Life cycle Relationship, Types of Digital Twin: Discrete Vs Composite, Product versus facility, Types of Digital Twin: Simulation versus operational, Analytics versus physics-based, Characteristics of a Digital Twin, Digital Twin Architecture, Industrial Digital Twin applications, Examples of mock, functional, and executable twins, Metaverse and Metaversity, About Azure Digital Twin, Azure Digital Twin Explorer, DTDL Models, Industry Ontologies, Setting up mixed reality DT using Azure DT in Unity, Build a 3D scene in Mixed Reality in Unity, Configure 3D assets for mixed reality in Unity, Connect IoT data to mixed reality with Azure Digital Twins and Unity, Connect IoT data to mixed reality with Azure Digital Twins and Unity

14 Hours

Unit 3: Digital Twin for Healthcare: Challenges, Digital twin models, DT architecture models, Case study: automatic remote surgeon using robot, DT and VR; Background and introduction, AI in DT models, Types of AI models in DT for health; DT in Cardiology- challenge heart diseases, cardiology future; Case Studies: Nutrition: HairLoss, Allergy: Anaphylaxis Shocks

14 Hours

Unit 4: Digital Twin & Cyber Security. : Digital twins and cybersecurity, Security Framework, Digital twins threat modelling, Common attacks on digital twins, Common attacks on digital twins, Digital twin authentication and identification challenge, IDS, IPS, Authentication Methods, Communication Channel Protection, Building cyber resilience in digital twins, Privacy Framework, Lack of Privacy, and trust, Privacy by Design, Enhancing trust with block chain integration.

12 Hours

Tools/ Languages: C/ C++/ JAVA/ Python using OpenGL.

Textbooks:

1. "Interactive Computer Graphics - A top-down approach with shader-based OpenGL", Edward Angel and Dave Shreiner, Pearson Education, Sixth edition, 2012.
2. Building Industrial Digital Twins by Shyam Varan Nath & Pieter van Schalkwyk, by Packt Publishing Ltd.

Reference Books

1. El Saddik, Abdulmotaleb, ed. *Digital Twin for Healthcare: Design, Challenges, and Solutions*. Elsevier, 2022.

Web References:

1. https://in.mathworks.com/campaigns/offers/next/digital-twins-for-predictive-maintenance/modeling-methods.html
2. https://learn.microsoft.com/en-us/training/paths/build-mixed-reality-azure-digital-twins-unity/

UE23CS842A: IoT FOR CONNECTED HEALTHCARE II

The Course will introduce the role of connected health applications, such as the Internet of Things (IoT), remote care, and disease and lifestyle management in facilitating more efficient and effective care and supporting the shift from hospital to community-based care. Connected Health and the Internet of Things will focus on exploring the variety of connected health technologies and solutions currently in use or emerging in the healthcare industry. They will provide you with the best practices for their successful adoption, integration, deployment, monitoring in clinical settings and the unique operational and privacy and security implications of these technologies.

Course Objectives:

- To learn how to design and implement IoMT applications that manages big data, streaming data, and/or distributed data.
- Equip participants with the knowledge and tools required to develop and execute strategies for adoption and integration of connected technologies in healthcare organizations.
- Enable participants to develop, measure, and monitor Key Performance Indicators related to the safe and effective use of connected health technologies.
- Apply best practices to ensure the security, privacy, and ethical use of connected health devices and data within regulated healthcare environments.

Course Outcomes:

Students will be able to-

- Demonstrate a comprehensive understanding of the foundations of the Internet of Medical Things (IoMT) and its significance in healthcare.
- Explain the fundamentals of wearable technologies and their role in connected healthcare.
- Select appropriate communication protocols for different healthcare scenarios.
- Create mathematical models for IoT-based healthcare monitoring systems, understanding the methodology and components involved.
- Understand IoT threats, vulnerabilities, and perform threat modeling and risk analysis.

UNIT1-Introduction to IoT & IoMT: IoMT is important for Healthcare, How IoMT is changing medicine, Benefits, challenges and opportunities, IoMT: Foundation and Characterization-IoMT and Robotics, Integration of Bio-interfaces, Devices and Sensors, Remote Health monitoring

10hrs

UNIT 2: Wearable Technologies & IoMT: Fundamentals of Wearable Technologies, Wearable Chemical and Biochemical Sensors. Technology of Connected Devices – Device Types, Sensors, Actuators. Internet of Things

– Devices, Objects, Physical Activity Modeling and Behavior Change. Internet of Things – Interface and Interaction Design, Human Body Communication for a Data Rate Sensor Network. Internet of Things – Networking, Wearable Sensors for Monitoring of Physical and Physiological Changes and for Early Detection of Diseases.

12hrs

UNIT 3: Communication Protocols: Application Layer Protocols**:** Message Queing Telemetry Transport, Constrained Application Protocol, Hyper Text Transfer Protocol; Network Layer Protocols: IPv4, WiFI, IEEE 802.15.4 Zigbee, Bluetooth Low Energy Protocol

10hrs

UNIT 4: Mathematical Modelling of IoT based Health Care Monitoring System: Modelling, Methodology and Component, Proposed System, How the Circuit Functions, Experimental Results, Mathematical Model Result on IoT HMS.

10hrs

UNIT5: IoT Security: IoT **–** Threats, Vulnerabilities, Threat Modelling and Risk, Security Regulations, Privacy Concerns and Regulations, Security and Privacy Examples, Threat Protection Methods, IoT and Blockchain.

12 hrs

Text Books:

1. David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Rob Barton and Jerome Henry, IoT Fundamentals: Networking Technologies, Protocols and Use Cases for Internet of Things, Cisco Press, 2017.

2. Edward Sazonov, Michael R. Neuman (editors), Wearable Sensors: Fundamentals, Implementation and Applications, 2014, Academic Press/Elsevier, ISBN 978-0124186620

3. Honbo Zhou, Internet of Things in the Cloud – A Middleware Perspective, 2012, CRC Press, ISBN 978-1439892992 .

4. Dian, F. John. Fundamentals of Internet of Things: For Students and Professionals. John Wiley & Sons, 2022.

Reference Books:

1. Li, Shancang, and Li Da Xu. Securing the internet of things. Syngress, 2017.

2. Hu, Fei. Security and privacy in Internet of things (IoTs): Models, Algorithms, and Implementations. CRC Press, 2016.

3. D. Jude Hemanth, J. Anitha, George A Tsihrintzis. IOMT: Remote Healthcare Systems and Applications. Springer, 2020.

4.Claire Rowland, Elizabeth Goodman, Martin Chalier, Ann Light, Alfred Lui, Designing Connected Products: UX for the Consumer Internet of Things, 2015, 60 O'Reilly Media,Inc, ISBN 978-1449372569