Nirma University

Institute of Technology

School of Technology

Department of Computer Science and Engineering

M Tech in Computer Science and Engineering
(Information and Network Security)

3CS1108 Advance Computer Networks [3 0 1 4]

Course Learning Outcome:
At the end of the course, students will be able to,

- understand the congestion control and queuing models in network
- demonstrate the knowledge of modern networking concepts and data center network planning
- apply the concepts learnt in this course to optimize performance of modern networks
- design and configure networks to support a specified set of applications

Syllabus:
Network Concepts: Introduction to Computer Networks, Networking Principles, Constant Bit Rate and Variable Bit Rate Network Services, Network Elements, Multiplexing, Switching, Error Control, Flow Control
Congestion Control: Performance of networks, delay and throughput, TCP congestion control, Analysis of TCP, QoS and fairness, traffic shaping and congestion control in TCP
Routing: Router scheduling algorithms, Router architectures, Border Routing protocols, MPLS
Software Defined Networking: Data Plane, Control Plane, Application Plane, Controller design, Virtualization, OpenFlow protocol for SDN, Network Function Virtualization
Data Center Networking: Data center architectures, Data center congestion control, queuing and traffic patterns, Data center network protocols, End host architectures, multipath TCP, Low Latency protocols for Data center, Load balancing
Applications: Distributed hash tables, Peer-to-peer systems, Content delivery networks, multimedia networks, Video streaming networks, Health networks, White Space Networking – WhiteFi

Self Study:
The self-study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self-study contents.

Laboratory Work:
Laboratory work will be based on above syllabus with minimum 8 experiments to be incorporated..

References:

1 William Stallings, Foundations of Modern Networking (SDN, NFV, QoE, IoT and Cloud), Pearson
2 William Stallings, High-speed networks and Internets – Performance and Quality of Service, PHI
3 James Kurose and Keith Ross, Computer Networking: A Top-Down Approach, Pearson
4 Hans W. Barz, Gregory A. Bassett, Multimedia Networks: Protocols, Design and Applications, Wiley

5 Rajkumar Buyya, Mukaddim Pathan and Athena Vakali, Content Delivery Networks, Springer
6 Relevant research papers for the topics

L	T	P	C
3	0	0	3

Course Code	3CS1113
Course Name	Applied Mathematics for Computer Science

Course Learning Outcomes (CLOs):
At the end of the course, students will be able to –

1. comprehend the mathematical fundamentals related to sets, probability, statistics, linear algebra and mathematical optimization
2. apply the mathematical principles to solve wide range of problems in computer science
3. use the mathematical concepts as per the need of the application

Syllabus:	Teaching Hours
Unit I	
Review of Linear Algebra: Matrices, Vectors properties, Eigenvalues and eigenvectors, Matrix factorizations, Distance measures, Projections, Notion of hyperplanes, Half-planes, Application for Linear Algebra in Computer Science	8
Unit II	
Probability, Statistics and Random Processes: Probability theory and axioms; Random variables; Probability distributions and density functions (univariate and multivariate), Expectations and moments, Covariance and correlation, Confidence intervals, Correlation functions, Random walks, Markov chains, Statistical inference, Applications in Regression and Classifications.	16
Unit III	
Optimization: Basic Concepts, Linear Programming, Duality, Constrained	12

and unconstrained optimization, gradient decent and non-gradient techniques, Introduction to least squares optimization, optimization in Practice.

Unit IV 9

Advanced topics: Nonlinear dimensionality reduction methods, PCA in high dimensions and random matrix theory (Marcenko-Pastur), Linear Discriminant Analysis, Non-Negative Matrix Factorization, Hypothesis testing, Proof Techniques, Random Graphs

Self-Study:

The self-study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self-study contents.

Suggested Readings^:

1. Gilbert Strang, Introduction to Linear Algebra, Cambridge Press.
2. Gilbert Strang, Linear Algebra and its applications, Harcourt, Brace, Jovanovich Publishers
3. Douglas C. Montgomery, George C. Runger, Applied Probability and Statistics for Engineers, Wiley
4. M. Mitzenmacher and E. Upfal, Probability and Computing: Randomized Algorithms and Probabilistic Analysis, Cambridge University Press
5. Sheldon Ross, A first course in Probability, Pearson
6. Cathy O'Neil and Rachel Schutt, Doing Data Science, O'Reilly Media
7. Avrim Blum, John Hopcroft, and RavindranKannan, Foundations of Data Science, e-book, Cornell University
8. Afonso S. Bandeira, Ten Lectures and Forty-Two Open Problems in the Mathematics of Data Science, e-book, MIT OCW
9. Jeff M. Phillips, Mathematical Foundations for Data Analysis, e-book, University of Utah
10. O. Paneerselvam, Operational Research, PHI

L=Lecture, T=Tutorial, P=Practical, C=Credit

^this is not an exhaustive list

L	T	P	C
3	0	2	4

Course Code	3CS1109
Course Title	Complexity Theory and Algorithms

Course Learning Outcomes (CLOs):
At the end of the course, students will be able to -

1. comprehend time & space complexity and formal aspects of algorithms
2. identify appropriate data structures and methodologies for efficient algorithm design
3. design and implement efficient algorithms using various approaches

Syllabus:	Teaching Hours:
Unit I Mathematical Preliminaries of computational complexity: Asymptotic Notations, Proof of correctness, Performance analysis, Recursive Algorithms and Recurrences	6
Unit II Complexity Theory: Various complexity classes, linear reductions. Probabilistic algorithms, Approximation algorithms and complexity classes relating to Parallel algorithms	8
Unit III Data Structures: Hash tables, Binomial heaps , Fibonacci heaps, Disjoint set structures	6
Unit IV Greedy Algorithms: Making change, graphs and minimum spanning tree, Shortest path, Knapsack problem, Scheduling, etc. Divide and Conquer: General Template, Various algorithm implementation like Binary search, Merge Sort, Quick Sort, Convex Hull, Matrix multiplication, etc.	12
Unit V Dynamic Programming: Introduction of Dynamic Programming, Principle of	6

Optimality, Examples like Single source shortest paths, Knapsack problem, Chained matrix multiplication, Longest Common Subsequence, etc.

Unit VI 7

Graph Algorithms: Elementary algorithms, DFS, BFS, Backtracking, and Branch & Bound techniques with related examples

Self-Study:

The self-study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self-study contents.

Laboratory Work:

Laboratory work will be based on above syllabus with minimum 10 experiments to be incorporated.

Suggested Readings^:

1. Gilles Brassard and Paul Bratley, Fundamentals of Algorithmics, PHI Publication.
2. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest& Clifford Stein, Introduction to Algorithms, PHI Publication.
3. Ellis Horowitz, SartajSahni, SanguthevarRajasekaran, Fundamentals of Computer Algorithms, University Press
4. Jean-Paul Tremblay and Paul G. Sorenson, An Introduction to Data Structures with Applications, Tata McGraw Hill
5. Robert L. Kruse, Data Structures and Program Design in C, PHI

L=Lecture, T=Tutorial, P=Practical, C=Credit

^this is not an exhaustive list

3CS1105 Comprehensive Assessment – I [0001]

Course Learning Outcome:

After successful completion of the course, student will be able to

- realize the collective understanding of various courses studied in the semester

Syllabus:

Student will be assessed on the basis of all the courses learned till end of the respective semester.

L	T	P	C
3	0	2	4

Course Code	3CS2107
Course Name	Cryptography

Course Learning Outcomes (CLO):
At the end of the course, students will be able to

1. understand the mathematical foundations to modern cryptographic techniques
2. critically evaluate symmetric and asymmetric cryptographic techniques
3. evaluate modern cryptographic techniques such as Digital Signatures and Hashing

Syllabus:	Teaching Hours
Unit I Cryptography:Basics of cryptography, OSI Security Architecture, Security attacks, services and mechanisms	3
Unit II Symmetric Ciphers: Introduction,Classical encryption techniques, Block ciphers and data encryption standards, Basic cryptanalysis, Modular arithmetic, Stream ciphers, AES algorithm	8
Unit III Block Cipher operations: Multiple encryptions and Triple DES, different modes of block cipher operations	4
Unit IV Pseudorandom number generation and stream ciphers: Principles of pseudorandom number generations, Pseudorandom number generators, Pseudorandom number generations using a block cipher, stream ciphers	4
Unit V Public key cryptosystem: Principles of public key cryptosystem, The RSA algorithm, Fermat's and Euler's theorem, Elliptic Curve Cryptography, Elgamal, other public key cryptosystems	5
Unit VI Cryptographic hash functions: Requirements and applications of cryptographic hash functions, Hash function based on Cipher Block	5

Chaining, Secure Hash Algorithm	
Unit VII	5
Message Authentication Codes: Requirements and applications of Message Authentication Codes, MACs based on Hash function, MACs based on Block ciphers	
Unit VIII	6
Digital Signatures: Requirements and Applications of Digital Signatures, different digital signature schemes	
Unit IX	5
Key Management and Distribution:Symmetric key distribution using symmetric encryption, Symmetric key distribution using asymmetric encryption, distribution of public keys	

Self-Study:
The self-study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self-study contents.
Laboratory Work:
Laboratory work will be based on above syllabus with minimum 10 experiments to be incorporated.
Suggested Readings:

1. W. Stallings, Cryptography and Network Security: Principles and Practices, Prentice Hall.
2. Charlie Kaufman, Network Security: Private Communication in a Public World, PHI.
3. Aegean Park Pr, Basic Cryptanalysis, Field Manual, DoD, USA.
4. J. Katz and Y. Lindell., Introduction to Modern Cryptography, Taylor & Francis.
5. A. Menezes, P. Van Oorschot, S. Vanstone, Handbook of Applied Cryptography, Taylor & Francis.

L=Lecture, T=Tutorial, P=Practical, C=Credit

^this is not an exhaustive list

3CS1103 Data Structure and Algorithms [3 0 1 4]

Course Learning Outcome:
After successful completion of the course, student will be able to

- **identify the appropriate data structure and algorithm design method for the given application**
- **evaluate various techniques for searching, sorting and recurrence**
- **analyze and design efficient algorithms**
- **calculate and conclude the associated algorithms' operations and complexity**

Syllabus:
Elementary Data Structures: Arrays, stack, queues, linked list, sorting techniques, Hash Tables,Binary Search Trees, B-Trees, Binomial heaps
Mathematical Preliminaries: Algorithm analysis, Algorithm Proof Techniques, Analysis ofAlgorithms
Growth of Functions: Analyzing Control Structures, Using a barometer, Average case analysis,Amortized Analysis, Solving recurrences
Greedy Algorithms: Making change, graphs and minimum spanning tree, knapsack problem,Scheduling
Divide and Conquer: General Template, various algorithm implementation eg Binary search , Heapsort, Quick Sort, Finding the median, matrix multiplication
Dynamic Programming: Introduction of Dynamic Programming, Principle of Optimality,Comparison with divide and conquer, single source shortest paths, Chained matrix multiplication
Graphs: Elementary Graph Algorithms, DFS, BFS, Backtracking, The knapsack problem, EightQueens problem, Branch and bound: The assignment problem
Computational Complexity and NP-Completeness: The classes of P and NP, Polynomialreductions, NP-complete problems, NP completeness proofs, NP hard problems, Non-Deterministicalgorithms

Self Study:
The self study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self study contents.

Laboratory Work:
Laboratory work will be based on above syllabus with minimum 5 experiments to be incorporated.

References:

1. Gilles Brassard and Paul Bratley, Fundamentals of Algorithmics, PHI
2. Thomas Cormen, Introduction to Algorithms, PHI
3. Trembly and Sorenson, Data Structure and Algorithms,PHI

3CS1101 High Speed Networks [3 - 1 4]

Learning Outcome

- Students would be able to describe and interpret the basics of high speed networking technologies.
- Students will be able to apply the concept learnt in this course to optimize and troubleshoot high-speed network.
- Students will be able to demonstrate the knowledge of network planning and optimization.
- Students will be able to design and configure network that have outcome characteristics needed to support a specified set of applications.

Syllabus

Introduction to Computer Networks, Networking Principles, Constant Bit Rate, Variable Bit Rate Network Services, Network Elements, Multiplexing, Switching, Error Control, Flow Control
Introduction to High Speed Networks, Analysis of Network traffic using deterministic and stochastic Models, Simulation tools, Tele-traffic engineering, Queuing Models
High Speed TCP Variants, Congestion Control in TCP/IP, ATM
High Speed LAN, Gigabit Ethernet, Distributed Queue Dual Bus (DQDB)
Protocols for QoS Support: IntServ, DiffServ, RSVP, MPLS
Optical Fiber Transmission, TCP/IP Performance over Optical Networks, Fiber Distributed Data Interface, Switched Multi-Megabit Dual Service(SMDS)
Applications demanding high speed communication, Multimedia IP broadcasting, Error resilience in Multimedia Transmission, Satellite Broadcasting

Self Learning Component

To be decided by course coordinator at the beginning of semester, which will be a blend of one or more of the e-Learning Resources, Video Lectures, Online courses, tools, research material, web links etc. along with the related assessment component(s).

Laboratory Work

Above concepts are to be implemented and at least 5 experiments are to be carried out.

References

1. High-speed networks and Internets – Performance and quality of service by William Stallings
2. High Performance TCP/IP Networking: Concepts, issues and solutions: By Mahoob Hassan Raj and Jain
3. High-speed networks: TCP/IP and ATM design principles by William Stallings
4. High speed networks by Marc Boisseau, Michel Demange, Jean-Marie Munier
5. Multimedia Communications: Applications, Networks, Protocols and Standards, Fred Halsall, Addison –Wesley

3CS2104 Mathematical Foundation for Network Security [3 1 0 4]

Course Learning Outcome:

After successful completion of the course, student will be able to

- understand the knowledge of basic mathematics related to research in networks
- apply the mathematics related to network in their projects and seminars
- apply concepts related to graphs for network optimization
- optimize performance of networks using graphs

Syllabus:

Linear Programming: Introduction, Formulation of LPP – Graphical Solution of LPP – Solution of LPP by simplex method – Mixed Constraints, Dual of Linear programming problem application of linear programming.

Finite fields: Groups, Rings and Fields, Modular Arithmetic, Euclidean Algorithm, Galois Field, Order of a group, Multiplicative group, Order of an Element in the group, Order of an element in multiplicative group, Generators, cyclic group, finding inverses, extended Euclidean Algorithm, Applications in RSA, Quadratic Residue and its applications

Introduction to Number Theory: Prime Numbers, Fermat's and Euler's Theorem, Testing for Primality, Chinese Remainder Problem

Number Theory Problems: Integer Fraction Problem, RSA Problem, Quadratic Residuosity Problem, Computing Square Roots in Z_n, Discrete Logarithm Problem, Diffie-Hellman Problem, Composite Moduli, Computing Individual bits, Subset sum problem, Factoring Polynomials over finite fields

Prime Number Issues: Probabilistic Primality Tests, Primality Tests, Irreducible polynomials over Z_P, Generators and elements of higher order

Random Numbers: Random and Pseudo Random Bit Generation, Statistical Tests, Cryptographically Secure pseudorandom number generation

Short path problems: Introduction to Shortest path problems, Method of finding the shortest path, Processing/balancing & Time Scheduling.

Graph Theory: Graph isomorphism, sub graphs, paths, reachability and connectedness, cycles, matrix representation of graphs, trees, labeled trees, tree searching, undirected trees, spanning trees of connected relations, minimal spanning trees, Vertex Cover Problem, Graph Coloring Problems, Min-cut Max-flow problems, Applications of Graph Theory in Network and Security

Self Study:
The self study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self study contents.

Tutorial Work:
Tutorial work will be based on above syllabus with minimum 10 tutorials to be incorporated.

References:

1 Kantiswarup and Manmohan Gupta, Operations Research, S.Chand& Sons
2 William Stallings, Cryptography and Network Security, PHI
3 S.D. Sharma, Operations Research, KedarnathRamnath& Co.
4 H.A. Tana, Operations Research, Prentice Hall
5 Tremblay J.P., Manohar R, Discrete Mathematical Structures with Applications to Computer Science, Tata McGraw-Hill
6 NarsinghDeo, Graph Theory with applications to Engineering and Computer Science, PHI
7 Alfred J Menezes, Paul C Van Oorschot and Scott Vanstone, E-book on Handbook of Applied Cryptography, CRC Press

Course Code	3CS2106
Course Name	System and Network Security

L	T	P	C
3	0	2	4

Course Learning Outcomes (CLOs):

At the end of the course, students will be able to –

1. identify the security basedvulnerabilities in operating systems and networks
2. illustrate the attacks on various operating systems and related prevention techniques
3. apply various defensive techniques to protect network based systems

Syllabus:	Teaching Hours:
Unit I **Detecting System Intrusions:** Monitoring key files, security objectives, 0 day attacks, good known state, rootkits, low hanging fruit, antivirus, homegrown intrusion detection, full packet capture devices, Out-of-band attack vectors, Security Awareness Training, Data Correlation, SIEM	**4**
Unit II **Preventing System Intrusions**: Sobering numbers, Bots, Symptoms of Intrusion, Security Policies, Risk Analysis, Controlling User Access, Intrusion Prevention Capabilities	**5**
Unit III **Guarding Against Network Intrusions:** Traditional Reconnaissance Attacks, Malicious Software, Defense in Depth, Preventive Measures, Intrusion Monitoring and detection, reactive measures	**6**
Unit IV **Unix and Linux Security:** Basic Unix Security Overview, Achieving Unix security, Protecting User Accounts and Strengthening Authentication, Limiting Super user Privileges, Securing Local and Network File Systems, Network Configuration, Improving security of Linux and Unix systems, Hardening Linux and Unix, Proactive Defense	**6**
Unit V **Internet Security**: Internet Protocol Architecture, Internet Threat Model, Defending against attacks on internet, Internet Security Checklist	**6**
Unit VI **Intranet and Local Area Network Security:** NAC and Access Control,	**12**

Measuring risks and audit, Authentication and Encryption, Wireless Network Security, Identify Network Threats, Establish Network Access Control, Risk Assessment, Listing Network Resources, Threats, Security Policies, Incident Handling Process, secure design through network access controls, Introducing IDS, NIDS and Firewall, Dynamic NAT configuration, Perimeter, Access list details, Packet Filtering, Monitor and Analyze System Traffic, Signature Analysis, Statistical Analysis, Signature Algorithms, Change Management, Physical and Environment Protection, Personnel Security, Information and System Integrity, Security Assessments, Risk Assessments

Unit VII **6**

Cellular Network, RFID, Optical and Wireless Security: Taxonomy and vulnerability analysis, RFID Challenges and Protections, Deployment Architectures for Optical and Wireless Security Implementation

Self Study:

The self-study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self-study contents.

Laboratory Work:

Laboratory work will be based on above syllabus with minimum 7 experiments to be incorporated.

Suggested Readings^:

1. Vacca, John R., Network and system security, Elsevier.
2. Pfleeger, C. P., &Pfleeger, S. L., Security in computing, Prentice Hall Professional Technical Reference.
3. Stallings, W., Brown, L., Bauer, M. D., &Bhattacharjee, A. K., Computer security: principles and practice, Pearson Education.
4. Parker, D. B., Computer security management, Reston Publishing Company.
5. Ford, W., Computer Communications Security: principles, standard protocols, and techniques, PTR Prentice Hall.

3CS2105 Web Security and Vulnerability assessment [3 0 1 4]

Course Learning Outcome:

After successful completion of the course, student will be able to

- understand the core concepts related to malware, hardware and software vulnerabilities and their causes
- exploit the vulnerabilities related to computer system and networks using state of the art tools and technologies
- correlate obvious vulnerabilities in the network and computer system

Syllabus:

Working of Hackers: Invading PCs, Script Kiddies, Working of Personal Hacker Protection

Working of Spyware and Antispyware: Introduction to Spywares, Detection Escapism, Invading Privacy, Hijacking home page and search pages, working of dialers, working of keyloggers and rootkits, following spyware money trail, working of anti-spyware

Websites and privacy: Working of Cookies, Web bugs, Websites, Websites building personal profiles

Dangers of Internet Search: Working of Google, Individual Know-how

Phishing Attacks: Working of Phishing, following phishing money trail, protection against phishing attacks

Zombies and Trojan Horses: Working of Zombies and Bot Networks, Working of Trojan Horses, Zombie Money Trail, Working of Zombie and Trojan Protection

Security Dangers in Browsers: Hackers exploit Networks, Protection against browser based attacks

Worms and viruses: Working of viruses and worms, antivirus software

Wi-Fi security dangers and protections: Working of Wi-Fi, Invading Wi-Fi Networks, hotspots, Evil Twin Hacks and Protections

Working of Spam: Dangers of spam, Hiding identity and identification, Working 1of Anti-spam software

Denial of Service Attacks and Protection

Virtual Private Networks, Web Blocking and Parental Controls, Personal Firewalls and Proxies

Vulnerability assessment: Nessus, OpenVAS, Nexpose, web application scanning tools
Penetration testing tools: Metasploit, Canvas, Writing custom exploits

Defense in Depth: Host-based and Network-based defenses (Firewalls, Intrusion Detection/Prevention)

Network analysis: TcpDump, Wireshark, Netflow
Securing and hardening systems: Bastille, CIS, MS Baseline

Incident response and investigation: Log review, Log management and correlation, incident response process and tools

Cloud security: Tools to assess and monitor cloud-based system security

Self-Study:
The self-study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self-study contents.

Laboratory Work:
Laboratory work will be based on above syllabus with minimum 10 experiments to be incorporated.

References:

1. Preston Galla, How Personal and Internet Security Work,Que Publications
2. Alfred Basta and Wolf Halton, Computer Security Concepts, Issues and Implementation, Cengage Learning
3. Shon Harris, Allen Harper, Chris Eagle and Jonathan Ness, Gray Hat Hacking: The Ethical Hackers' Handbook, TMH Edition
4. Jon Erickson, Hacking: The Art of Exploitation, SPD
5. Peltier, T. R., Peltier, J., & Blackley, J. A. (2003). *Managing a Network Vulnerability Assessment*. CRC Press.
6. Caswell, B., Beale, J., Ramirez, G., & Rathaus, N. (2005). *Nessus, Snort, and Ethereal Power Tools:* Customizing Open Source Security Applications. Elsevier.

L	T	P	C
3	0	2	4

Course Code	3CS1111
Course Name	Applied Machine Learning

Course Learning Outcomes (CLOs):

At the end of the course, students will be able to –

1. comprehend statistical methods as basis of machine learning domain
2. apply and evaluate variety of machine learning algorithms
3. implement machine learning techniques to solve problems in interdisciplinary domains

Syllabus:	Teaching Hours
Unit I Introduction: Motivation and Applications, Basics of Supervised and Unsupervised Learning	3
Unit II Regression Techniques: Basic Concepts and applications of Regression, Simple Linear Regression – Gradient Descent and Normal Equation Method, Multiple Linear Regression, Non-Linear Regression, Linear Regression with Regularization, Hyper-parameters tuning, Loss Functions, Decision Tree Regression, Evaluation Measures for Regression Techniques	13
Unit III Classification Techniques: Naïve Bayes Classification: Fitting Multivariate Bernoulli Distribution, Gaussian Distribution and Multinomial Distribution, K-Nearest Neighbours, Classification Trees, Linear Discriminant Analysis, Support Vector Machines: Hard Margin and Soft Margin, Kernels and Kernel Trick, Evaluation Measures for Classification Techniques	10
Unit IV Artificial Neural Networks: Biological Neurons and Biological Neural Networks, Perceptron Learning, Activation Functions, Multilayer Perceptrons, Back-propagation Neural Networks, Learning with Momentum, Winner-take-all Learning, Competitive Neural Networks,	9

Adaptive ANN

Unit V 4

Clustering: Hierarchical Agglomerative Clustering, k-means Algorithm, Self-Organizing Maps

Unit VI 6

Advances in Machine Learning:Basics of Semi-Supervised and Reinforcement Learning, Introduction to Deep Learning, Best Practices for Machine Learning, Case Studies in interdisciplinary domain

Self-Study:

The self-study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self-study contents.

Laboratory Work:

Laboratory work will be based on above syllabus with minimum 5 experiments to be incorporated.

Suggested Readings^:

1. C. Bishop, Pattern Recognition and Machine Learning, Springer
2. R. O. Duda, P. E. Hart and D. G. Stork, Pattern Classification and Scene Analysis, Wiley
3. KishanMehrotra, Chilukuri Mohan and Sanjay Ranka, Elements of Artificial Neural Networks, Penram International
4. Tom Mitchell, Machine Learning, TMH
5. RajjanShinghal, Pattern Recognition, Techniques and Applications, OXFORD
6. AthemEalpaydin, Introduction to Machine Learning, PHI
7. Andries P. Engelbrecht, Computational Intelligence - An Introduction, Wiley Publication
8. Andrew Kelleher, Adam Kelleher, Applied Machine Learning for Data Scientist and Software engineers, Addison-Wesley Professional

3CS1E28 Artificial Intelligence [3 0 1 4]

Course Learning Outcome:
After successful completion of this course, student will be able to

- understand concept of knowledge representation and predicate logic and transform the real life information in different representation
- understand state space and its searching strategies
- analyze a system and its implementation

Syllabus:
Introduction to Artificial Intelligence Overview: What is AI, Importance, and early work in AI, AI related fields.
Knowledge: General concepts, definition and importance of knowledge, knowledge based system, representation, organization, manipulation and acquisition of knowledge.
Problems, Problem Spaces and State Space Search: The AI Problems, The Underlying Assumption, What Is An AI Techniques, The Level Of The Model, Criteria For Success, Some General References, One Final Word. Defining The Problems As a State Space Search, Production Systems, Production Characteristics, Production System Characteristics, and Issues In The Design Of Search Programs.
Knowledge Representation: Knowledge Representation Issues, Representations And Mappings, Approaches to knowledge Representation, Using Predicate Logic Representation Simple Facts in Logic, Representing Instance and ISA Relationships, Computable Functions And Predicates, Resolution. Representing Knowledge Using Rules, Procedural Versus Declarative Knowledge, Logic Programming, Forward Versus Backward Reasoning.
Weak Slot-And-Filler Structure : Semantic Nets, Frames.
Search and Control Strategies : Uninformed(Blind) and informed search, DFS, BFS, Heuristic Search Techniques : Generate-And-Test, Hill Climbing, Best-First Search, A*, AO*, Problem Reduction, Constraint Satisfaction, Means-Ends Analysis.
Reasoning : Symbolic Reasoning Under Uncertainty, Introduction to Non-monotonic Reasoning, Logics for Non-monotonic Reasoning. Statistical Reasoning , Probability And Bay's Theorem, Certainty Factors And Rule-Base Systems, Bayesian Networks, Dempster-Shafer Theory.
Game Playing: Overview and Example Domain, Min-max Search, Adding Alpha-Beta Cutoffs.

Expert System: Introduction, Architecture, and Types of Expert Systems.

Self Study:
The self study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self study contents.

Laboratory Work**:**
Laboratory work will be based on above syllabus with minimum 5 experiments to be incorporated.

References:

1 Elaine Rich And Kevin Knight, Artificial Intelligence and Expert Systems, Tata McGraw-Hill.
2 D.W.Patterson, Artificial Intelligence and Expert System, Development, W.Rolston, Mcgraw-Hill International Edition.
3 Ivan Bratko, Introduction to Prolog Programming Carl Townsend PROLOG Programming for Artificial Intelligence, Addison-Wesley
4 ClocksinAndMellish, "Programming with PROLOG", Stuart Russell.
5 Peter Norvig, Artificial Intelligence: A Modern Approach, Prentice Hall.

L	T	P	C
3	0	2	4

Course Code	3CS12D301
Course Name	Big Data Systems

Course Learning Outcomes (CLOs):
At the end of the course, students will be able to

1. analyse the big data analytic techniques for business applications.
2. manage big data using different tools and frameworks.
3. design efficient algorithms for mining the data from large volumes.
4. implement the HADOOP and MapReduce technologies associated with big data analytics

Syllabus	Teaching Hours
Unit I Introduction to Big Data: Introduction to Big Data Platform, Challenges of Conventional Systems, Intelligent Data Analysis, Nature of Data, Analytic Processes and Tools, Analysis vs Reporting, Modern Data Analytic Tools, Statistical Concepts: Sampling Distributions, Re-Sampling, Statistical Inference - Prediction Error	5
Unit II The Big data technology landscape : NoSQL, Types of No SQL databases, SQL Vs No SQL, why No SQL, Introduction to MongoDB, Data Types in MongoDB, CRUD, Practice examples, Apache Cassandra, Features of Cassandra, CRUD operations	10
Unit III Hadoop: History of Hadoop, The Hadoop Distributed File System, Components of Hadoop, Analysing the Data with Hadoop, Scaling Out, Hadoop Streaming, Design of HDFS, Java Interfaces to DFS Basics, Developing a Map Reduce Application, How Map Reduce Works,	10

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

Unit IV 10

Hadoop Environment: Setting up a Hadoop Cluster, Cluster Specification, Cluster Setup and Installation, Hadoop Configuration, Security in Hadoop, Administering Hadoop, HDFS, Monitoring, Maintenance, Hadoop benchmarks, Hadoop in the Cloud.

Unit IV 10

Frameworks: Applications on Big Data Using Pig and Hive, Data Processing Operators in Pig, Hive Services, HiveQL, Querying Data in Hive, Fundamentals of HBase and ZooKeeper, IBM Info Sphere Big Insights and Streams, Visualizations, Visual Data Analysis Techniques, Interaction Techniques, Systems and Applications

Self-Study:

The self-study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self-study contents.

Laboratory Work:

Laboratory work will be based on above syllabus with minimum 6 experiments to be incorporated.

Suggested Readings^:

1. Michael Berthold, David J. Hand, Intelligent Data Analysis, Springer
2. Tom White, Hadoop: The Definitive Guide, Third Edition, O'reilly Media
3. Chris Eaton, Dirk DeRoos, Tom Deutsch, George Lapis, Paul Zikopoulos, Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data, McGraw Hill Publishing
4. Anand Rajaraman and Jeffrey David Ullman, Mining of Massive Datasets, Cambridge University Press
5. Bill Franks, Taming the Big Data Tidal Wave: Finding Opportunities in Huge Data Streams with Advanced Analytics, John Wiley & sons

6. Glenn J. Myatt, Making Sense of Data, John Wiley & Sons
7. Pete Warden, Big Data Glossary, O'Reilly
8. Jiawei Han, Micheline Kamber, Data Mining Concepts and Techniques, Second Edition, Elsevier
9. Da Ruan, Guoquing Chen, Etienne E. Kerre, Geert Wets, Intelligent Data Mining, Springer
10. Paul Zikopoulos, Dirk deRoos, Krishnan Parasuraman, Thomas Deutsch, James Giles, David Corrigan, Harness the Power of Big Data: The IBM Big Data Platform, Tata McGraw Hill Publications
11. Michael Minelli, Michele Chambers, Ambiga Dhiraj, Big Data, Big Analytics: Emerging Business Intelligence and Analytic Trends for Today's Businesses, Wiley Publications
12. Zikopoulos, Paul, Chris Eaton, Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data, Tata McGraw Hill Publications
13. Seema Acharya and Subhashini C, Big Data and Analytics, Wiley India

L=Lecture, T=Tutorial, P=Practical, C=Credit

L	T	P	C
2	0	2	3

Course Code	3CS12D201
Course Name	Blockchain Technology

Course Learning Outcomes (CLOs):
At the end of the course, students will be able to

1. comprehend the structure of a Blockchain networks
2. evaluate security issues relating to Blockchain and cryptocurrency
3. design and analyze the applications based on Blockchain technology

Syllabus:	Teaching Hours
Unit I Introduction to Blockchain: History, Digital Money to Distributed Ledgers, Design Primitives, Protocols, Security, Consensus, Permissions, Privacy	3
Unit II Blockchain Architecture, Design and Consensus: Basic crypto primitives: Hash, Signature, Hashchain to Blockchain, Basic consensus mechanisms, Requirements for the consensus protocols, PoW and PoS, Scalability aspects of Blockchain consensus protocols	8
Unit III Permissioned and Public Blockchains: Design goals, Consensus protocols for Permissioned Blockchains, Hyperledger Fabric, Decomposing the consensus process, Hyperledger fabric components, Smart Contracts, Chain code design, Hybrid models (PoS and PoW)	9
Unit IV Blockchain cryptography: Different techniques for Blockchain cryptography, privacy and security of Blockchain, multi-sig concept	6

Unit V 4

Recent trends and research issues in Blockhain: Scalability, secure cryptographic protocols on Blockchain, mltiparty communication, FinTech and Blockchain applicabilities

Self-Study:
The self-study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self-study contents.

Laboratory Work:
Laboratory work will be based on above syllabus with minimum 5 experiments to be incorporated.

Suggested Readings^:

1. Narayanan, Arvind,. et al, Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press.
2. Wattenhofer, Roger, The science of the blockchain, CreateSpace Independent Publishing Platform
3. Bahga, Arshdeep, and Vijay Madisetti,. Blockchain Applications: A Hands-on Approach, VPT
4. Nakamoto, Satoshi, Bitcoin: A peer-to-peer electronic cash system, Research Paper
5. Antonopoulos, Andreas M, Mastering Bitcoin: Programming the open blockchain, O'Reilly Media, Inc
6. Diedrich, Henning, Ethereum: Blockchains, digital assets, smart contracts, decentralized autonomous organizations, Wildfire Publishing (Sydney)

L=Lecture, T=Tutorial, P=Practical, C=Credit

3CS1E13 Cloud Computing [3 0 1 4]

Course Learning Outcome:
After successful completion of this course, student will be able to

- describe the hardware and software concepts and architecture of cloud computing
- contrast the key technical and commercial issues concerning cloud computing versus traditional software models
- recognize the importance of virtualization technology in support of cloud computing
- explore the issues related to cloud computing data centres

Syllabus:
Foundations: Distributed system models and enabling technologies, computer clusters for scalable Computing, Introduction to Cloud Computing, On the Management of Virtual Machines for Cloud Infrastructures, Migrating to the cloud, virtual machines and virtualization of clusters and datacenters, Applications of Virtual Machines, Nested Virtualization
Cloud services: Infrastructure as a service, Virtual Machines Provisioning and Migration Services, Platform as a service , Enhancing Cloud Computing Environments
Using a Cluster as a Service, Software as a Service, SLA Management in Cloud Computing, Performance Prediction for HPC on Clouds, Workflow Engine for Clouds, Understanding Scientific Applications for Cloud Environments, The MapReduce Programming Model and Implementations,
Monitoring and Management of Cloud: A Service Provider's Perspective, Best PracticesinArchitecting Cloud Applications, Building Content Delivery Networks Using Clouds,Resource Cloud Mashups,Security in cloud, Governance and Case Studies, Legal Issues in Cloud Computing, Achieving Production Readiness for Cloud Services Exploring prototypes and present day clouds.

Self Study:
The self study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self study contents.

Laboratory Work:
Laboratory work will be based on above syllabus with minimum 5 experiments to be

incorporated.

References:

1. RajkumarBuyya, James Broberg,Andrzej M Goscinski, Cloud Computing: Principles and Paradigms, Wiley Publication.
2. Kai Hwang, Jack Dongarra& Geoffrey C. Fox, Distributed and Cloud Computing: Clusters, Grids, Clouds and the Future Internet, Elsevier
3. Gautam Shroff, Enterprise Cloud Computing: Technology, Architecture, and Applications, Cambridge University Pres
4. Toby Velte, Anthony Velte, Cloud Computing, A Practical Approach, McGraw-Hill Osborne Media, McGraw-Hill
5. Selected Research Papers from Various Sources.

3CS1205 Comprehensive Assessment – II [000 1]

After successful completion of the course, student will be able to

- realize the collective understanding of various courses studied in the semester

Syllabus:
Student will be assessed on the basis of all the courses learned till end of the respective semester.

3CS2203 Cyber Security and Laws [3 0 1 4]

Course Learning Outcome:

After successful completion of the course, student will be able to

- realize the activities carried using forensic technologies in detection of cyber crime
- introduce a novel methodology of performing cyber forensics or system forensics
- relate the laws enforced by the judiciary to handle cybercrimes and cyber frauds
- assess how the digital evidences will be handled in any crime scene

Syllabus:

Computer and Cyber Forensic Basics:Introduction to Computers, Computer History, Software, Hardware, Classification, Computer Input-Output Devices, Windows, DOS Prompt Commands, Basic Computer Terminology, Internet, Networking, Computer Storage, Cell Phone / Mobile Forensics, Computer Ethics and Application Programs, Cyber Forensic Basics-Introduction to Cyber Forensics, Storage Fundamentals, File System Concepts, Data Recovery, Operating System Software and Basic Terminology Data and Evidence Recovery:Introduction to Deleted File Recovery, Formatted Partition Recovery, Data Recovery Tools, Data Recovery Procedures and Ethics, Preserve and safely handle original media, Document a "Chain of Custody", Complete time line analysis of computer files based on file creation, file modification and file access, Recover Internet Usage Data, Recover Swap Files/Temporary Files/Cache Files, Introduction to Encase Forensic Edition, Forensic Tool Kit (FTK), Use computer forensics software tools to cross validate findings in computer evidence-related cases.
Cyber Crimes and Cyber Laws:Introduction to IT laws & Cyber Crimes – Internet, Hacking, Cracking, Viruses, Virus Attacks, Pornography, Software Piracy, Intellectual property, Legal System of Information Technology, Social Engineering, Mail Bombs, Bug Exploits, and Cyber Security
Cyber Forensics Investigation:Introduction to Cyber Forensic Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Encryption and Decryption methods, Search and Seizure of Computers, Recovering deletedevidences, Password Cracking

Cyber Security: Introduction to Cyber Security, Implementing Hardware Based Security, Software Based Firewalls, Security Standards, Assessing Threat Levels, Forming an Incident Response Team, Reporting Cyber crime, Operating System Attacks, Application Attacks, Reverse Engineering & Cracking Techniques and Financial Frauds

Security Audit and Standards: Risk Assessment and Management, Asset Classification, Crisis Management Plan, Resources Recovery Strategy, Security Testing, International Standards, Analysis and Logging, Security Certification

Self Study:
The self study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self study contents.

Laboratory Work:
Laboratory work will be based on above syllabus with minimum 5 experiments to be incorporated.

References:

1. Raghu Santanam, Sethumadhavan, MohitVirendra, Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives, IGI Global
2. Chris Davis, IT Auditing Using controls to protect Information Assets, TMH

L	T	P	C
3	0	2	4

Course Code	3CS12D103
Course Name	Data Privacy

Course Learning Outcomes (CLOs):
At the end of the course, students will be able to –

1. comprehend the concepts of web security and privacy, hardware and software vulnerabilities and protection mechanisms
2. realize the need for data privacy and the related technologies
3. derive and demonstrate the protection mechanisms against several data related attacks

Syllabus: Teaching Hours

Unit I 10

Introduction to Security: Cryptography, Web security, Hardware and software vulnerabilities

Unit II 10

Data Privacy: Data localization issues, Managing personally identifiable or sensitive information, Hippocratic databases, Differential privacy, Privacy preserving data analysis

Unit III 5

Basic concepts and definitions, objectives, disclosure control and inference of entities, models of protection like null map, k-map, wrong-map

Unit IV 10

Data Explosion: Availability vs. Storage vs. Collection trade-off, barriers to distribution, mathematical models for sharing practices and policies for computing privacy and risk measurements

Unit V 10

Demographics and Uniqueness, data linking, data profiling, data privacy attacks

Self-Study:

The self-study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self-study contents.

Laboratory Work:

Laboratory work will be based on above syllabus with minimum 7 experiments to be incorporated.

Suggested Readings^:

1. Stallings, W. Cryptography and Network Security. Pearson Education India.
2. Giannotti, F., &Pedreschi, D. (Eds.). Mobility, data mining and privacy: Geographic knowledge discovery. Springer Science & Business Media.
3. Bygrave, L. A. Data privacy law: an international perspective (Vol. 63). Oxford: Oxford University Press.
4. Scoble, R., Israel, S., &Benioff, M. R.. Age of context: Mobile, sensors, data and the future of privacy. USA: Patrick Brewster Press.
5. Bendat, J. S., &Piersol, A. G. Random data analysis and measurement procedures.

3CS1E23 Data Warehousing and Mining [3 0 1 4]

Course Learning Outcome:
After successful completion of this course, student will be able to

- identify the key processes of data mining, data warehousing and knowledge discovery process
- understand the basic principles and algorithms used in practical data mining and their strengths and weaknesses
- apply data mining techniques to solve problems in other disciplines in a mathematical way

Syllabus:
Introduction, Multidimensional Data Model, Data Warehouse & OLAP Technology for Data Mining, Architecture, Differences of Data warehouse and Data mart, Data Preprocessing, Preprocessing Techniques, Data Mining Primitive, Language & System Architecture.
Concept Description: Characterization and Comparison, Attribute Oriented Induction.
Mining Association rules in large database, Techniques for frequent pattern mining.
Classification & Prediction: Classifier, ID3, C4.5, Regression. Cluster analysis, clustering techniques.
Applications of Mining
Intelligent Functionalities of Warehouse: Querying and Reporting, Online Analytical Processing, Data mining and Executive information systems (EIS).
Case study of some available OLAP tools.

Self Study:
The self study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self study contents.

Laboratory Work**:**
Laboratory work will be based on above syllabus with minimum 5 experiments to be incorporated.

References:
1 Jiahei Han &MichelineKamber, Data Mining Concepts and Techniques, Morgan

Kaufmann
2 S. Nagabhushana, Data Warehousing OLAP and Data Mining, New Age publishers

L	T	P	C
2	0	2	3

Course Code	3CS2205
Course Name	Digital Forensics, Audit and Investigation

Course Learning Outcomes (CLOs):
At the end of the course, students will be able to

1. identify the need of digital forensic and role of digital evidences
2. illustrate forensic duplication and file system analysis
3. apply network forensics to collect digital evidences

Syllabus: Teaching Hours

Unit I 2
Introduction to Ethical Hacking: Difference between Hacking and Ethical hacking, Steps of Ethical Hacking, Tools for ethical hacking

Unit II 2
Introduction to Cyber Crime: Types of cybercrime, categories of cybercrime , Computers' roles in crimes, Prevention from cyber-crime, Hackers, Crackers, Phreakers

Unit III 3
Digital Forensics and Digital Evidences: Rules for Digital Forensic, The Need for Digital Forensics, Types of Digital Forensics, Ethics in Digital Forensics, Types of digital evidences and their characteristics, Challenges in digital evidence handling

Unit IV 6
Computer Security Incident Response: Introduction to Computer Security Incident, Goals of Incident response, Incident Response Methodology,

Formulating Response Strategy, Incidence Response Process, Data Collection on Unix based systems

Unit V 2

Forensic Duplication: Forensic Image Formats, Traditional Duplication, Live System Duplication, Forensic Duplication tools

Unit VI 4

Disk and File System Analysis: Media Analysis Concepts, File System Abstraction Model, Partition Identification and Recovery, Virtual Machine Disk Images , Forensic Containers Hashing, Carving, Forensic Imaging

Unit VII 2

Data Analysis: Data Analysis Methodology, Investigating Applications, Malware Handling

Unit VIII 3

Network Forensics: Technical Exploits and Password Cracking, Analyzing Network Traffic, Collecting Network based evidence, Evidence Handling, Investigating Routers, Handling Router Table Manipulation Incidents, Using Routers as Response Tools

Unit IX 3

Forensic Investigation Report: Goals and Layout of an Investigative Report, guidelines for writing a Report, method(s) to write a forensic report.

Unit X 3

Forensic Tools: Need and types of computer forensic tools, tasks performed by computer forensic tools, Study of different tools to acquire, search, analyze and store digital evidence

Self-Study:
The self-study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self-study contents.

Laboratory Work:

Laboratory work will be based on above syllabus with minimum 5 experiments to be incorporated.

Suggested Readings^:

1. Jason Luttgens, Matthew Pepe, Kevin Mandia, Incident Response and computer forensics, Tata McGraw Hill.
2. Nilakshi Jain, Dhananjay Kalbande, Digital Forensic: The fascinating world of Digital Evidences, Wiley India Pvt Ltd.
3. Cory Altheide, Harlan Carvey, Digital forensics with open source tools, Syngress Publishing, Inc.
4. Chris McNab, Network Security Assessment, O'Reily.
5. Clint P Garrison, Digital Forensics for Network, Internet, and Cloud Computing A forensic evidence guide for moving targets and data, Syngress Publishing, Inc.
6. Bill Nelson, Amelia Phillips, Christopher Steuart, Guide to Computer Forensics and Investigations, Cengage Learning
7. Debra Littlejohn Shinder Michael Cross Scene of the Cybercrime: Computer Forensics Handbook, Syngress Publishing, Inc.
8. Marjie T. Britz, Computer Forensics and Cyber Crime, Pearson, Preston Galla, How Personal and Internet Security Work, Que Publications

L=Lecture, T=Tutorial, P=Practical, C=Credit

^ This is not an exhaustive list

L	T	P	C
3	0	2	4

Course Code	3CS22D302
Course Name	Ethical Hacking

Course Learning Outcomes (CLOs):
At the end of the course, students will be able to

1. comprehend the core concepts related to malware, hardware and software vulnerabilities and their causes
2. realize the ethics behind hacking and vulnerability disclosure
3. exploit the vulnerabilities related to the computer systems and networks using state of the art tools and technologies

Syllabus:	Teaching Hours
Unit I Introduction to Ethical Disclosure:Ethics of Ethical Hacking, Ethical Hacking, and the legal system, Proper and Ethical Disclosure	5
Unit II Computer devices Hacking: Basic Overview of Kali Linux, Server side attacks, Client side attack, command-line shell scripting	8
Unit III Network Hacking: Information gathering, wire, and wireless packet sniffing, ARP and DNS spoofing, MITM attacks, Detection, and Security	10
Unit IV Website Hacking: Information gathering, OWASP Vulnerabilities and discovery of Vulnerabilities using open source tools	8
Unit V	6

Defence in Depth: Host-based and Network-based defenses (Firewalls, Intrusion Detection/Prevention)

Unit VI 8

Hardware security: Digital System Design Sequential System Specification, Vulnerabilities in Digital Logic Design, watermarking , Side channel attack and counter measures, Hardware Trojan detection, FPGA system security

Self-Study:
The self-study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self-study contents.

Laboratory Work:
Laboratory work will be based on above syllabus with minimum 10 experiments to be incorporated.

Suggested Readings^:

1. Preston Galla, How Personal and Internet Security Work, Que Publications
2. Alfred Basta and Wolf Halton, Computer Security Concepts, Issues and Implementation, Cengage Learning
3. Shon Harris, Allen Harper, Chris Eagle and Jonathan Ness, Gray Hat Hacking: The Ethical Hackers' Handbook, TMH Edition
4. Jon Erickson, Hacking: The Art of Exploitation, SPD
5. Peltier, T. R., Peltier, J., Blackley, J. A. Managing a Network Vulnerability Assessment, CRC Press.
6. Caswell, B., Beale, J., Ramirez, G., Rathaus, N. Nessus, Snort, and Ethereal Power Tools: Customizing Open Source Security Applications, Elsevier.

L=Lecture, T=Tutorial, P=Practical, C=Credit

^this is not an exhaustive list

L	T	P	C
3	0	2	4

Course Code	3CS12D104
Course Name	Internet of Things

Course Learning Outcomes (CLOs):
At the end of the course, students will be able to

1. comprehend the architectural components and platforms of IoT ecosystem
2. apply appropriate access technology and protocol as per the application requirement
3. identify data analytics and data visualization tools as per the problem characteristics

Syllabus:	Teaching Hours
Unit I	
Introduction, applications, need and scope of IoT, Various IoT architectures, functional stack, Processors and Operating Systems for resource constrained devices	5
Unit II	
Sensors and actuators, smart objects, Connecting objects, protocols and access technologies like IEEE802.15.4, LFNBPLC, LoRaWAN, WirelessHART, LTE-M, BLE, NB-IoT, Sigfox, White-Fi and HaLow	12
Unit III	
IoT network layer, IPv6: IPv6 structure, addressing, routing, interconnecting issues, 6LoWPAN: forwarding, addressing, header compression, neighbour discovery, Routing in LLN, RPL	7
Unit IV	
Application layer protocols, CoAP, MQTT, AMQP, XMPP, Integrating Internet Services with Interoperable data encoding with XML, JSON and CBOR, Sensor data models and representation, The Sensor Mark-up Language (SENML), lightweight web services for IoT	9
Unit V	

Data analytics for IoT, machine learning, big data analytics tools and technology like NoSQL, Hadoop	5
Unit VI	
Securing IoT, Challenges in IoT security, provisions for securing IoT network	4
Unit VII	
Case studies on IoT applications: Connected Vehicles, Autonomous Vehicles, Industrial Applications of IoT	3

Self-Study:

The self-study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self-study contents.

Laboratory Work:

Laboratory work will be based on above syllabus with minimum 6 experiments to be incorporated.

Suggested Readings^:

1. David Hanes, G. Salgueiro, IoT Fundamentals - Networking Technologies, Protocols, and Use Cases for Internet of Things, Cisco Press
2. Jean-Philippe Vasseur, Adam Dunkels, Interconnecting Smart Objects with IP: The Next Internet, Morgan Kaufmann
3. Pethuru Raj, Anupama Raman, The Internet of Things - Enabling Technologies, Platforms and Use Cases, CRC Press
4. Robert Stackowiak, Art Licht, VenuMantha and Louis Nagode, Big Data and The Internet of Things, Apress
5. Peter Waher, Learning Internet of Things, Packt Publishing Ltd
6. Daniel Kellmereit, Daniel Obodovski, The Silent Intelligence: The Internet of Things, DND Ventures
7. Olivier Hersent, David Boswarthick, Omar Elloumi, The Internet of Things: Key Applications and Protocols, Wiley Publications

L=Lecture, T=Tutorial, P=Practical, C=Credit

^this is not an exhaustive list

3CS2204 Intrusion Detection Systems [3 0 1 4]

Course Learning Outcome:

After successful completion of the course, student will be able to

- realize the research aspects in the field of intrusion detection systems
- optimize performance of detection systems by employing various machine learning techniques
- apply knowledge of machine learning in system and network protection
- devise various research projects in the area of IDS for all sorts of networks

Syllabus:

Approaches in Anomaly based Intrusion Detection Systems: Introduction, Payload based vs. header based approaches, setting up an ABS, PAYL & POSEIDON, Conclusions

Formal Specification for Fast Automatic Profiling of Program Behavior: Introduction, Related Works, Methodology, Case Study, Remus configuration and conclusions

Learning Behavior Profiles from Noisy Sequences: Introduction, Learning by abstraction, Regular Expressions, String Alignment and Flexible Matching, Learning Algorithm, Evaluation of Artificial Traces, User Profiling

Correlation Analysis of Intrusion Alerts: Introduction, Approaches based on similarity between Alert Attributes, approaches based on predefined attack scenarios, approaches based on prerequisites and consequences of attacks, approaches based on multiple information sources, Privacy issues in auto correlation

An approach to preventing, correlating, predicting multi-step network attacks: Introduction, Related work, preliminaries, Hardening network to prevent multistep intrusions, Correlating and predicting multiple steps attacks

Response: Bridging the link between Intrusion Detection alerts and security policies: Security Policy Formalism, Threat Response system, From alerts to new policies

Intrusion Detection and Reaction: An integrated approach to network security: Proposed Framework, Architecture for Intrusion Detection, Intrusion reactions, attack sessions, intrusion detection subsystem, traffic classification and intrusion reaction, testing

Self Study:

The self study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self study contents.

Laboratory Work:
Laboratory work will be based on above syllabus with minimum 5 experiments to be incorporated.

References:

1 Roberto Di Pietro and Luigi Mancini, Intrusion Detection Systems, Springer
2 Rafeeq Ur Rehman, Intrusion Detection Systems with Snort, Pearson Education, Prentice Hall
3 Guide to Intrusion Detection and Prevention Systems, National Institute of Science and Technology

Course Code	3CS2206
Course Title	Minor Project

Course Outcomes (COs):

At the end of the course, students will be able to -

1. identify the issues related with the recent trends in the field of computer science and its applications
2. formulate the problem definition, analyze and do functional simulation of the same
3. design, implement, test and verify the proposed solution related to problem definition
4. compile, comprehend and present the work carried out

A student is required to carry out project work in the relevant area of post-graduate study. The project may include design / simulation / synthesis / development of a system, etc. At the end of the semester, a student has to submit a detailed report incorporating literature survey, problem formulation, clear problem statement, research methods, result analysis, conclusion, etc. It is expected that the student should defend his/her work before the jury / panel of examiners.

L = Lecture, T = Tutorial, P = Practical, C = Credit

3CS1E07 Modern Databases [3 0 1 4]

Course Learning Outcome:
After successful completion of this course, student will be able to

- understand query processing and optimization for various centralized / distributed databases
- understand new-generation data models used for highly distributed databases
- design and deploy various column oriented, document oriented, key-value stores and graph databases
- apply tools and techniques for applications related to social networks and similar systems

Syllabus:
Principles of query processing, Indexing techniques, Query execution plans and operators, Query optimization Next-generation data models, Aggregate Data Models ,declarative query language, Distribution Models
Databases Vs. File Systems: GFS, HDFS, Big Data, Bigtable/HBASE Row-oriented Vs. column-oriented storage Advanced indexing methods, Scalable data processing , Parallel query plans and operators, massively parallel joins
Systems based on MapReduce: Hadoop, Hive
Scalable Key-Value Stores: Amazon Dynamo, Cassandra No-SQL Databases, Document Store database
Distributed Data:Parallel Computing with Monad algebra, NESL, DryadLINQ, PigLatin Graph Databases, Grid & Cloud Database Solutions Large-Scale Graph Processing: Pregel

Self Study:
The self study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self study contents.

Laboratory Work:
Laboratory work will be based on above syllabus with minimum 5 experiments to be incorporated.

References:
1. Martin Fowler, Pramod J. Sadalage,NoSQL Distilled, Pearson.

2. Elmasri and Navathe,Fundamentals of Database Systems, 6th Ed Addison Wesley.
3. Garcia-Molina, Ullman and Widom, Database Systems: The Complete Book, Pearson.
4. Connolly and Begg, Database Systems, Addison Wesley.
5. J. Hellerstein& M. Stonebraker,THE RED BOOK: Readings in Database Systems, MIT Press.
6. Selected research papers relevant to the course topics

3CS1201 Research Seminar [0 0 1 1]

Course Learning Outcome:

After successful completion of the course, student will be able to

- compare the work done by various researchers in the area of interest using literature survey
- identify the research gaps in the specific area of interest
- demonstrate practical aspect of research contribution
- comprehend and document the study and contributionmadetowards research

Syllabus:

Candidates have to select any Research Topic as Self Study for their Research Seminar. They will be required to present the progress of their Study in front of the Reviewing Panel at Regular intervals. During the final review, student are required to submit the report of Seminar.

3CS1E33 Secured Wireless Communications [3 0 1 4]

Course Learning Outcome:
After successful completion of this course, student will be able to

- understand the fundamental concepts of wireless network and wireless network security
- understand how the performance of wireless networks depends on factors such as the protocols used, and assess the role of communication standards in wireless communication system
- identify WLAN security issues and design a strategy to manage WLAN security ensuring confidentiality of data flowing over WLAN network thereby adhering to ethics in wireless network safety
- examine the various known security risks associated with implementing wireless networks and demonstrate tools to identify the security breaches and analyze wireless security

Syllabus:
Security in General Wireless/Mobile Networks: High Performance Elliptic Curve Cryptographic Co-processor, An Adaptive Encryption Protocol in Mobile Computing
Security in Ad Hoc Network: Pre-authentication and authentication models in Ad Hoc Networks, Promoting Identity – based key management in Wireless Ad Hoc Networks, A survey of attacks and countermeasures in mobile ad hoc networks, Secure routing in Wireless Ad Hoc Networks, Survey of IDS in Ad Hoc Networks Security in Mobile Cellular Networks
Security in Wireless LANs: Cross Domain Mobility Adaptive Authentication, AAA Architecture and Authentication for wireless LAN Roaming, Experimental Study on Security Protocols in WLANs
Security in Sensor Networks: Security Issues, Key Management Schemes, Secure Routing in Ad Hoc and Sensor Networks

Self Study:
The self study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self study contents.

Laboratory Work**:**

Laboratory work will be based on above syllabus with minimum 5 experiments to be incorporated.

References:

1 Y. Xiao, X. Shen, D. Z.Du, Wireless Network Security, Springer International Edition.

3CS1E34 Securing High Performance Computing Environment [3 0 1 4]

Course Learning Outcome:
After successful completion of this course, student will be able to

- understand the area of information and network security through the high end computing standards like cluster computing, cloud computing and grid computing
- develop an insight into the high end processing capabilities of nodes
- analyze scientific applications needing multiple cores
- identify highly useable and cost efficient cloud computing capabilities to meet national scale requirements for new modes of computationally intensive scientific research

Syllabus:
Introduction, need and general purpose issues of high performance computing. Overview of Various HPC Systems, Techniques for achieving security in multi-user computer systems, Security problems in computing,
Security in Distributed Computing - Security and content distribution networks, Key management and agreement in Distributed systems, Security in Autonomic Computing
Security in Cloud Computing - Introduction to Cloud Computing, concepts of security in Cloud, Cloud security challenges, Infrastructure security, Data security and storage in Cloud, data dispersal techniques, High-availability and integrity layer for cloud storage , Encryption and key management in the cloud , Cloud forensics , Data security and Storage, Data location and availability, Data security tools and techniques for the Cloud, Trustworthy Cloud infrastructures , Secure computations , Cloud related regulatory and compliance issues, Prototypes of Cloud service providers.
Security in Grid Computing - Grid Security Architecture and Infrastructure, Standards and Models for Grid Security, Trust based access control management framework for a secured grid environment, Single Sign-On, Unifying grid and organizational security mechanisms

Self Study:
The self study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self study contents.

Laboratory Work**:**
Laboratory work will be based on above syllabus with minimum 5 experiments to be incorporated.

References:

1. Mather, T., Kumaraswamy S., and Latif, S. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media.
2. Terrence V Lillard, Digital Forensics for Network, Internet, and Cloud Computing: A Forensic Evidence Guide for Moving Targets and Data, Syngress Publication.
3. Charles P Pfleeger, Shari Lawrence Pfleeger, Security in Computing, Prentice Hall.
4. Yang Xiao, Security in Distributed, Grid, Mobile, and Pervasive Computing,Auerbach Publications.
5. John Rittinqhouse, James Ransome. Cloud Computing, Implementation, Management and Security, CRC Press.

3CS2201 Securing Interconnecting Systems [2 0 2 4]

Course Learning Outcome:

After successful completion of the course, student will be able to

- understand the basics of interconnecting and securing devices
- identify security threats on the network and study various solutions
- select appropriate tools and technologies to identify and rectify the security loopholes
- design secured network by configuring various elements of networks and devices

Syllabus:

Introduction to System Interconnection- Planning-Establishing-Maintaining-Disconnecting Interconnect Systems, Enterprise Systems - Heterogeneous and Interdependent

Resilience of the Internet Interconnection Ecosystem-Resilience and Efficiency, Service Level Agreements, Reachability, Traffic and Performance, Regulation

Network Security and building- Security insurance policies, Security Triangle, Responding to security incident, Methods of network attacks, Evaluating network security, Disaster recovery considerations

Constructing a comprehensive network security policy, Threat and vulnerability analysis, Implementation of controls and safeguard, Traffic/Log analysis, Audit planning and techniques

Securing Routers - authentication, authorization, Accounting, Detailed router auditing

Securing Switches - protecting layer2 switches, VLAN hopping, Switch spoofing, STP attacks, DHCP server spoofing, Port Security

Firewalls - ACL, Traffic Filtering and traffic inspection,Alerts and audit trails, Security zones, Zone firewall policies

Intrusion Prevention System (IPS) and Intrusion detection Systems (IDS)- Detection methods, Network-based Vs Host-based IPS, IDS and IPS appliances, Alarms

Securing Storage Area Networks- Overview of SAN, Fundamentals and benefits, SAN security fundamentals, SAN Attacks, SAN Security Technologies

Securing VOIP-enabled Networks - Defining VOIP, VOIP benefits, VOIP Network, VOIP network Components and VOIP protocols, Common voice vulnerabilities, Securing VOIP Network

Self Study:
The self study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self study contents.

Laboratory Work:
Laboratory work will be based on above syllabus with minimum 5 experiments to be incorporated.

References:

1 CCSDS guide for secure system interconnection, NIST
2 Eric Maiwald, Fundamentals of Network and Security, TMH
3 CCNA Security Official Exam Certification Guide, Cisco Press
4 Various Research papers

3CS1E25 Semantic Web [3 0 1 4]

Course Learning Outcomes

After successful completion of this course, student will be able to

- understand the principles behind semantic web and Ontology Engineering
- model and design ontologies using Resource Description Framework (RDF) and Web Ontology Language (OWL)
- query ontologies using SPARQL
- apply semantic web technologies to real world applications

Syllabus

History, Semantic Web Layers, Semantic Web technologies, Semantics in Semantic Web

XML: Structuring, Namespaces, Addressing, Querying, Processing, Metadata, Traditional Search vs. Semantic Search

RDF and Semantic Web: RDF Specification , RDF Syntax, XML and Non-XML, RDF elements, RDF Relationship, Reification, Container and Collaboration , RDF Schema, Editing, Parsing, and Browsing RDF/XML, RQL, RDQL, SPARQL, Web Data Management,

Ontology: Ontology Movement, OWL, OWL Specification, OWL Elements, OWL Constructs, Simple and Complex, Ontology Engineering, Constructing Ontologies, Reusing ontologies, Ontology Reasoners, On To Knowledge Semantic Web architecture, Ontology Mapping, Alignment and Merging Tools, Ontology Editor

Logic and Inference: Logic, Description Logics, Rules, Monotonic Rules, Syntax, Semantics and Examples, Non Monotonic Rules, Motivation, Syntax, and Examples, Rule Markup in XML, Monotonic Rules and Non Monotonic Rules

Applications of Semantic Web Technologies: Commercial and Non Commercial Use of RDF, Sample Ontology, Web Services, Web Mining, Horizontal information, Data Integration, Future of Semantic Web

Self-Learning Component

To be decided by course coordinator at the beginning of semester, which will be a blend of one or more of the e-Learning Resources, Video Lectures, Online courses, tools, research material, web links etc. along with the related assessment component(s).

Laboratory Work
Above concepts are to be implemented and at least 5 experiments are to be carried out.

References

1. Grigorous Antoniou and Van Hermelen, A Semantic Web Primer, The MIT Press.
2. Dieter Fensel, Jim Hendler, Henry Lieberman and Wolfgang Wahister, Spinning the Semantic Web: Bringing the World Wide Web to Its Full Potential, The MIT Press.
3. Shelley Powers, Practical RDF, O'Reilly Publishers.
4. Manish Joshi, Harold Boley, Rajendra Akerkar, Advances in Semantic Computing, Techno Mathematics Research Foundation
5. Elliotte Rusty Harold, The XML 1.1 Bible, Wiley.

3CS1E04 Software Testing and Quality Assurance [3 0 1 4]

Course Learning Outcome:
After successful completion of this course, student will be able to

- learn and develop project documentations and soft skills for effective project presentation
- develop practical skills related to software quality assurance
- apply software testing techniques for information systems development

Syllabus:
Software Quality, Role of testing, verification and validation, White-Box and Black-Box Testing , Test Planning and Design, Monitoring and Measuring Test Execution, Test Tools and Automation, Test Team Organization and Management.
Unit Testing: Concept of Unit Testing, Static Unit Testing, Defect Prevention, Mutation Testing, Debugging, Unit Testing in eXtreme Programming
Control Flow Testing: Control Flow Graph, Paths in a Control Flow Graph, All-Path Coverage Criterion, Statement Coverage Criterion, Branch Coverage Criterion, Examples of Test Data Selection.
Data Flow Testing: Data Flow Anomaly, Data Flow Graph, Data Flow Testing Criteria, Feasible Paths and Test Selection Criteria, Comparison of Testing Techniques.
System Integration Testing: Types of Interfaces and Interface Errors, System Integration Techniques, Software and Hardware Integration, Off-the-Shelf Component Testing, Built-in Testing
System Test Categories: Basic Tests, Functionality Tests, Robustness Tests, Interoperability Tests, Performance Tests, Scalability Tests, Stress Tests, Load and Stability Tests, Reliability Tests, Regression Tests, Documentation Tests.
Functional Testing: Equivalence Class Partitioning, Boundary Value Analysis, Decision Tables, Random Testing, Error Guessing, Category Partition.
System Test Design: Test Design Factors, Requirement Identification, Characteristics of Testable Requirements, Test Design Preparedness Metrics, Test Case Design Effectiveness
System Test Planning and Automation: Structure of a System Test Plan, System Test Automation
System Test Execution: Metrics for Tracking System Test, Beta Testing, System Test Report, Product Sustaining, Measuring Test Effectiveness.

Acceptance Testing: Types of Acceptance Testing, Selection of Acceptance Criteria, Acceptance Test Execution, Acceptance Testing in eXtreme Programming.
Software Quality: Five Views of Software Quality, McCall's Quality Factors and Criteria, Quality Factors Quality Criteria, Relationship between Quality Factors and Criteria, Quality Metrics, ISO 9126 Quality Characteristics, ISO 9000:2000 Software Quality Standard ISO 9000:2000 Fundamentals, ISO 9001:2000 Requirements

Self Study:
The self study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self study contents.

Laboratory Work:
Laboratory work will be based on above syllabus with minimum 5 experiments to be incorporated.

References:

1. SagarNaik University of Waterloo, PiyuTripathy, Software Testing and Quality Assurance: Theory and Practice, Wiley.
2. William Perry, Effective Methods for Software Testing, Wiley.
3. Paul C. Jorgensen,Software Testing - A Craftsman's Approach, CRC Press.
4. Srinivasan Desikan and GopalaswamyRamesh,Software Testing, Pearson Education.
5. Louis Tamres,Introducing to Software Testing, Addison Wesley Publications.
6. Ron Patton, SAMS Techmedia Indian Edition,Software Testing, Pearson Education.
7. Glenford J. Myers,The Art of Software Testing, John Wiley & Sons.
8. Robert V. Binder, Testing Object-Oriented Systems: Models Patterns and Tools, Addison Wesley.
9. Daniel Galin, Software Quality Assurance, Pearson Education.

3CS1E24 Web Search and Mining [3 0 1 4]

Course Learning Outcome:
After successful completion of this course, student will be able to

- identify and differentiate between application areas for web content mining, web structure mining and web usage mining
- understand how web search engines crawl, index, and rank web content
- understand the functionality of the various web search and web mining methods and components

Syllabus:
Introduction to web mining, Taxonomy of web mining, Architecture of a general purpose web search engine such as google or alta vista Web Content Mining: document indexing and retrieval in the web environment - Boolean and vector retrieval models, latent semantic indexing (LSI), results ordering, meta-search, Indexing and Retrieval, Standard and extended query languages for web data. Indexing and retrieving text files by words. Database structure. Measuring the relevance of a text to a query, web documents categorization and clustering
Natural Language Processing Methods Used For Web Information Retrieval: lemmatization, part-of-speech tagging, disambiguation, shallow syntactic parsing etc.
Web Structure Mining: primary web browsing (crawling, spidering),focused crowling, link topology analysis, PageRank, HITS methods ,Global analysis of the Web
Social Networks Analysis Web Usage Mining: mining for user behavior on the web, internet marketing, Information Extraction as a specific type of web content mining: wrapper-based vs. token activated extraction
Specific Applications: opinion mining vs. fact mining, web spam analysis, comparative shopping, etc. Web information integration, mapping schemas usage
Web Mining And Its Relation To The Semantic Web: automatic semantic annotation, ontology learning, Semantic Web search The invisible web and specialized search engines.

Self Study:
The self study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self study contents.

Laboratory Work**:**
Laboratory work will be based on above syllabus with minimum 5 experiments to be incorporated.

References

1. SoumenCharkabarti, Mining The Web: Discovering Knowledge from Hypertext Data, Morgan Kaufmann.
2. RichardoBaeza-Yates and BerthierRibierno-Neto, Modern Information RetrievalAddison Wesley.
3. Alfred and Emily Glossbrenner, Search Engines for The World Wide Web, Peachpit Press.

3CS1301 **Project Part I** **[00 30 13]**

Course Learning Outcome:

After successful completion of the course, student will be able to

- compare the work done by various researchers in the area of interest using literature survey
- identify specific research gaps
- correlate other facets of research through innovative thinking and ideas
- demonstrate effective communication skills
- apply optimization and enhancement skillsforeffective research
- employ ethical practicesforresearch

Syllabus:

The student will carry out a project with significant technical contribution either in the institute, any R&D organization or Industry. At the end of the semester III, student will submit a report on the progress of his work.

3CS1401 **Project Part II** **[00 30 14]**

Course Learning Outcome:

After successful completion of the course, student will be able to

- compare the work done by various researchers in the area of interest using literature survey
- identify specific research gaps
- correlate other facets of research through innovative thinking and ideas
- demonstrate effective communication skills
- apply optimization and enhancement skills for effective research
- employ ethical practices for research

Syllabus:

The student will continue the project work started in semester III and complete the work defined and submit final dissertation for evaluation.