DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING, MIT, MANIPAL

M.TECH in COMPUTER SCIENCE & INFORMATION SECURITY

Course Structure (Applicable to 2016-17 admission onwards)

Year	FRIST SEMESTER						SECOND SEMESTER					
I	**Sub Code**	**Subject Name**	**L**	**T**	**P**	**C**	**Sub Code**	**Subject Name**	**L**	**T**	**P**	**C**
	MAT 5108	Computational Methods and Stochastic Processes	3	1	0	4	CSE 5221	Design of Secure Protocols	3	0	2	4
	CSE 5101	Advanced Data Structures and Algorithms	3	0	2	4	CSE 5222	Network Security	4	0	0	4
	CSE 5102	Advanced Data Base Systems	3	0	2	4	CSE****	Elective I	4	0	0	4
	CSE 5103	Advanced Computer Networks	3	0	2	4	CSE****	Elective II	4	0	0	4
	CSE 5121	Number Theory & Cryptography	3	0	2	4	CSE****	Elective III	4	0	0	4
	HUM 5101	Research Methodology and Technical Presentation	1	0	3	2	*** ****	Open Elective	3	0	0	3
	CSE 5112	Information Systems Lab I	0	0	6	2	CSE 5212	Information Systems Lab II	0	0	6	2
							CSE 5299	Technical Seminar	0	0	3	1
	Total		**16**	**1**	**17**	**24**	**Total**		**22**	**0**	**11**	**26**
II	**THIRD AND FOURTH SEMESTERS**											
	CSE 6099	Project Work							0	0	0	25
		Total							**0**	**0**	**0**	**25**

Programme Electives

1.	CSE 5233	Big Data Analytics
2.	CSE 5234	Cloud Computing
3.	CSE 5236	Data Mining & Applications
4.	CSE 5241	Secure E-Commerce
5.	CSE 5244	Web Services
6.	CSE 5245	Agent Systems and Security
7.	CSE 5246	Biometric Security
8.	CSE 5247	Cyber Security Standards and Best Practices
9.	CSE 5248	Database and Application Security
10.	CSE 5249	Information Security Management
11.	CSE 5250	Intrusion Detection Systems
12.	CSE 5251	Legal issues in Information Security
13.	CSE 5252	Mobile and Wireless Security
14.	CSE 5253	Object Oriented System Design
15.	CSE 5254	PKI and Trust Management

Open Electives

1.	CSE 5281	Information Storage and Management
2.	CSE 5282	Multicore program optimization

DEPT. OF COMPUTER SCIENCE & ENGG.

COURSE CONTENT FOR M.TECH (CSIS) 2016

MAT 5108 COMPUTATIONAL METHODS AND STOCHASTIC PROCESSES [3 1 0 4]

Probability : random variables, distribution, Bayesian estimation, credible intervals, Bayesian hypothesis, introduction to Stochastic Processes, Statistics of Stochastic Processes, correlation and covariance, stationary, autocorrelation, power density spectrum, Markov models, Gaussian mixture models, Data analysis, regression, predicting real value outputs. Optimization techniques: Mathematical formulation of linear programming problems, simplex method. Advanced Numerical Methods: Numerical solutions of BVP's by finite difference and finite element methods. Solution of parabolic elliptic, hyperbolic PDE's, Linear Algebra: Eigen values, eigen vectors, matrix computation and singular value decomposition methods. Graph theory: Basics of Graph Theory, connectivity, spanning tree and traversability.

References:

1. A Papoulis and S.U.Pillai, "*Probability, Random Variables and Stochastic Processos*", McGraw Hill 2002.
2. P.Z.Peebles Jr., "*Probability, Random Variables and Random Signal Principles*", McGraw Hill, International Edition, 2001 Singapore.
3. "*Applied Numerical Methods*", McGraw Hill.
4. Hamdy A.Taha, "*Operations Research*" McGraw Hill.
5. Frank Harary, "*Graph Theory*", Narosa Publishing House 2001.
6. Narasingh Deo "*Graph Theory with Applications to Engg. and Computer Science*", PHI Learning Pvt.Ltd.

CSE 5101 ADVANCED DATA STRUCTURES AND ALGORITHMS [3 0 2 4]

Amortized Analysis - Aggregate analysis, The accounting method, The potential method, Dynamic Tables B-Trees - Definition of B-Trees, Basic operations on B-Trees, Deleting a key from a B-Tree. Binomial Heaps - Binomial trees and Binomial heaps, Operations on Binomial heaps. Fibonacci Heaps - Structure of Fibonacci heaps, Mergeable heap opetions, Decreasing a key and deleting a node. van Emde Roas Trees, Data structures for Disjoint sets – Disjoint-set operations, Linked-list representation of disjoint sets, Disjoint set forests. Single-source Shortest Paths - The Bellman-Ford algorithm, Single-source shortest paths in directed acyclic graphs, Difference constraints and shortest paths, All-Pairs Shortest Paths - Shortest Paths and matrix multiplication, Johnson's algorithm for sparse graphs, Maximum Flow - Flow Networks, The Ford-Fulkerson method, Multithreaded Algorithms - The basics of dynamic multithreading , Multithreaded matrix multiplication , Multithreaded merge sort

References:

1. Cormen Thomas H., Leiserson Charles E, Rivest Ronald L. and Stein Clifford, *“Introduction to* Algorithms” *(3e),* MIT Press, 2009.
2. Cormen Thomas H., Leiserson Charles E, Rivest Ronald L. and Stein Clifford, “*Introduction to Algorithms” (2e),* Prentice-Hall India, 2001.
3. Baase Sara and Gelder A.V., *“Computer Algorithms -Introduction to Design and Analysis”, (3e),* Pearson Education, 2000.
4. Anany Levitin, *“Introduction to the Design and Analysis of Algorithms “, (3e),* Pearson Education, 2011.
5. Aaron M. Tenenbaum,Yedidyah Langsam,Moshe J. Augeustein, *”Data Structures using C”,* Pearson Education, 1998.

CSE 5102 ADVANCED DATA BASE SYSTEMS [3 0 2 4]

Advanced SQL Recursive Queries, Advanced Aggregation Features, SQL Performance Tuning, Query Processing and Optimization- Measures of Query Cost, Selection, Sort and Join Operations, Evaluation of Expressions, Transformation of Relational Expressions, Choice of Evaluation of Plans, Object based Databases - Complex Data Types, SQL3, Parallel Databases - Interquery, Intraquery, Intraoperation and Interoperation Parallelisms. Distributed Databases - data storage, Transactions, Commit Protocols, Concurrency Control, Availability, Query Processing, Data Warehouse – Multidimensional Modeling, OLAP, Semi Structured Data - Structure of XML data, schema, Querying and Transformation, Storage of XML data, MapReduce - Massive Data sets and Distributed File Systems, MapReduce algorithms for Relational algebra Operations, NoSQL – Data Models, Consistency, Implementation

References:

1. Silberschatz, Korth and Sudarshan, “*Database System Concepts”, (6e),* McGraw Hill, 2011.
2. Pramod J Sadalage , Martin Fowler, “*NoSQL Distilled: A Brief Guide to the Emerging World of Polyglot Persistence”, (1e),* Addison-Wesley , 2012.
3. Anand Rajaraman and Jeffrey David Ullman, “*Mining of Massive Datasets”, (6e),* Cambridge University Press, 2011.

CSE 5103 ADVANCED COMPUTER NETWORKS [3 0 2 4]

Need for DNS, Name spaces, Domains, Inverse Domain, Registrar, Resolution, Resolver, Mapping , Recursive Resolution, Iterative Resolution, Caching. Time-Sharing Environment, Network Virtual Terminal (NVT), Embedding, Options, Symmetry, Negotiation, Controlling the Server, Out-of-Band Signaling, Escape Character, Modes of Operation, User Interface, Security Issue. FTP Connections, Communication, Command Processing, Anonymous FTP. HTTP Transaction, Conditional Request, Persistence, Cookies, Caching, Proxy Server. Understanding Software Defined Networking(SDN, SDN facilitates server virtualization and cloud networks, Looking at the Benefits and Use Cases of SDN: SDN Automation, A new approach to network policy, Centralized policy management, Some Popular Use Cases for Deploying SDN, Expanding Beyond the Network and the Data Center. SDN Controllers, Policies, Overlay Networks, Automating Cloud via SDN. Key SDN Considerations and Requirements. Open Protocols, Open Architectures, Open Ecosystems, and Open Source. Programming Rather than Managing Manually, Easier Policy Implementation, Supporting Multivendor Ecosystems, Extensible Architecture, Open Source SDN Platform. Multimedia Networking Applications, Types of Multimedia, Streaming, DASH. Content Distribution Networks, Case Studies. Voice-over-IP. Best-Effort Service, Jitter, Protocols for Real-Time Applications, Best-Effort Networks, Quality-of-Service (QoS) Guarantees, Resource Reservation, Call Admission**.** Optical Networks: Multiplexing Techniques. Generations. Optical Packet Switching, Wavelength Standards, Optical Power and Loss. SONET/SDH: Multiplexing, VCAT and LCAS. Multiprotocol Label Switching, Carrier Transport. Resilient Packet Ring, QOS, WDM Network Elements. Optical Line Terminals, Amplifiers, Multiplexers, OADM Architectures, Concepts, Protection in SONET/SDH, Resilient Packet Rings, MPLS. Service Classes.

References:

1. Behrouz A. Forouzan, "*TCP/IP Protocol Suite*", *(4e),* McGraw-Hill, 2010.
2. Brian Underdahl and Gary Kinghorn, Software Defined Networking For Dummies, Cisco Special Edition, John Wiley & Sons, Inc., 2015.
3. James F. Kurose, Keith W. Ross, "*Computer Networking-A Top Down Approach*", *(6e)* Edition, Pearson, 2013.
4. Rajiv Ramaswami, Kumar N. Sivarajan, Galen H. Sasaki, "*Optical Networks -A Practical Perspective*", *(3e),* Morgan Kaufmann, 2010.

CSE 5121 NUMBER THEORY & CRYPTOGRAPHY [3 0 2 4]

Introduction, Modern Cryptography, Elements of Number Theory, Algebraic Structures in Computing, Complexity of Computing. Private Key Cryptosystems Classical ciphers, DES family, Modern private key cryptographic algorithms. Public Key Cryptosystems, RSA cryptosystems, Elliptic curve cryptosystems, Probabilistic encryption. Basic quantum theory, Introduction to quantum cryptography, 3B84, B92 protocols, Pseudorandomness, Number generators, Polynomial indistinguishability, RSA Pseudorandom bit generators, next bit test, Pseudorandom function generators, Pseudorandom permutation generators, Super pseudo random permutation generators. Hashing, Properties of hashing, Birthday paradox, Serial and parallel hashing, Hashing based on Cryptosystems, MD5, Keyed hashing. Digital Signatures Properties of digital signatures, Generic signature schemes, RSA signatures, Blind signatures, Undeniable signatures, Fail-stop signatures, Timestamping. Authentication Active opponents, Model of authentication systems. Interactive proof systems, perfect Zero-Knowledge proofs,

References:

1. J. Pieprzyk, T. Hardjono and J. Seberry, "*Fundamentals of Computer Security*", Springer International Edition, 2003.
2. Lawrence C. Washington, "*Elliptic curves: number theory and cryptography*", Chapman & Hall/ CRC Second Edition, 2008
3. Noson S. Yanofsky. Micro A. Mannucci, , "*Quantum Computing for Computer Scientists"*, Cambridge University Press, 2008
4. S. Vaudenay, "*A Classical Introduction to Cryptography: Applications for Communications Security*", Springer International Edition, 2006.
5. N. Koblitz, "*Course on Number Theory and Cryptography*", Springer Verlag 2006.

HUM 5101 RESEARCH METHODOLOGIES AND TECHNICAL COMMUNICATION

[1 0 3 2]

Mechanics of Research Methodology - Types of Research, Significance of research, Research framework, Case study method, Experimental method, Sources of data, Data collection using questionnaire, Interviewing and experimentation. Research formulation-Components, selection and formulation of a research problem, Objectives of formulation, and Criteria of a good research problem. Research hypothesis – Criterion for hypotheses construction, Nature of hypotheses, need for having a working hypothesis, Characteristics and Types of hypothesis, Procedure of hypotheses testing. Sampling Methods Introduction to various sampling methods and their applications. Data Analysis–Sources of data, Collection of data, Measurement and scaling technique, and Different techniques of Data analysis. Thesis Writing and Journal Publication-Writing thesis, Writing journal and conference papers, IEEE and Harvard styles of referencing, Effective presentation, Copyrights, and avoiding plagiarism.

References:

1. Dr.Ranjit Kumar, "*Research Methodology: A Step-by-Step Guide for Beginners*", SAGE,2005

2. Geoffrey R. Marczyk, David DeMatteo & David Festinger, "*Essentials of Research Design and Methodology*", John Wiley & Sons, 2004.
3. John W.Creswel, "*Research Design : Qualitative, Quantitative, and Mixed Methods Approaches*", SAGE 2004
4. Suresh C.Sinha and Anil K.Dhiman, "*Research Methodology (2 Vols-Set)",*Vedam Books, 2006.
5. C.R.Kothari, "*Research Methodology: Methods and Techniques*", New Age International Publisher, 2008.

CSE- 5112 INFORMATION SYSTEMS LAB I

[0 0 6 2]

Experiments/mini project based on the syllabus specified in first semester.

CSE 5221 DESIGN OF SECURE PROTOCOLS [3 0 2 4]

Introduction To Cryptography Protocol, Information Security And Cryptography, Classes Of Cryptographic Protocols, Security Of Cryptographic Protocols, Background Of Cryptographic Protocols Preliminaries, Cryptographic Primitives, Cryptographic Protocols, Security Of Cryptographic Protocols, Communication Threat Model, Engineering Principles For Security Design Of Protocols, Introduction Of Engineering Principles, Protocol Engineering Requirement Analysis, Detailed Protocol Design, Provable Security, Informal Analysis Schemes Of Cryptographic Protocols, Guarantee Of Cryptographic Protocol Security, Formalism Of Protocol Security Analysis, Design Cryptographic Protocol Based On Trusted Freshness, Previously Known Method For Protocol Design, Security Properties To Achieve In Protocol Design, Application Of Protocol Design Via Trusted Freshness

References:

1. Ling Dong and Kafei Chen, "*Cryptographic Protocol: Security Analysis based on trusted Freshness"*, Springer, 2012
2. Bruce Schneier, **"***Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C", (2e),* Wiley Computer Publishing, John, Wiley & Sons, Inc, 1996.
3. Alfred J. Menezes, Paul C. Van Oorschot and Scott A Vanstone, "*Handbook of Applied Cryptography"*, CRC press, 2001.
4. Wenbo Mao, "*Modren Cryptography: Theory and Practice", (5e)*, Pearson Education, 2004.
5. Michael R. A. Huth, "*Secure Communicating Systems: Design, Analysis and Implementation"*, Cambridge University Press, 2001
6. P. Y. A. Ryan, S. A. Schneider, M. H. Goldsmith, G. Loweand A. W. Roscoe, "*The modeling and analysis of security protocols"*, Pearson Education, 2010.

CSE 5222 NETWORK SECURITY [4 0 0 4]

Security Attacks, Types of Attacks, Security Services, Security Mechanisms, A Model of Network Security. Genesis of Computer Viruses, Classification of Infection Strategies, Classification of In-Memory Strategies, Basic Self-Protection Strategies, and Classification According to Payload, Antivirus Defense Techniques, Firewalls, Types of Firewall security Policy, Firewall Types, Intrusion Detection and Prevention:,Intrusion Detection, Intrusion Detection System(IDS),Types of Intrusion Detection Systems, Intrusion Prevention systems, IPsec, IKE phases, Phase 1 IKE, Phase 2/Quick Mode, Traffic selectors, IKE Phase 1 protocols, Phase-2 IKE: Setting up IPsec's SAs, ISAKMP/IKE Encoding, VPN, SSL/TLS protocol, Exportability, Encoding, PGP , S/MIME, HTTPS, SET, Security in Link Layer and over LANs. Kerberos V4, and Kerberos V5

References:

1. Chalie Kaufman, Radia Perlman, Mike Speciner, "*Network Security : PRIVATE Communication in a PUBLIC World", (2e),* Pearson Education, 2005
2. Peter Szor, *"The art of Computer Virus Research and Defense", (1e),* Addison Wesley Professional,2005
3. John R.Vacca, Scott Ellis, "*Firewall Jumpstart for Network and System Administrators", (1e),* Elsevier Digital Press, 2005
4. Joseph Migga Kizza, "*Guide to Computer Security", (3e),* Springer,2015
5. William Stallings, "*Cryptography and Network Security Principles and Practice"*, (6e), Prentice Hall, 2014

CSE-5212 INFORMATION SYSTEMS LAB-II

[0 0 6 2]

Experiments/mini project based on the syllabus specified in second semester

CSE-5299 TECHNICAL SEMINAR
[0 0 3 1]

Each student has to present a seminar individually, on any technical topic related to the subject, but not covered in the syllabus. The time duration for presentation is 45 minutes and 15 minutes is devoted for question and answer session. Slides have to be prepared for the presentation. A seminar report has to be submitted one week before the day of the presentation.
Ref. Materials : IEEE transactions, Technical journals, Proceedings of National and International Conferences, Web sites.

III/IV SEMESTER

CSE-6099 PROJECT WORK [0 0 0 25]

The duration of this major project is one year. Students are required to undertake innovative and research oriented projects, which not only reflect their knowledge gained in the previous two semesters but also reflects additional knowledge gained from their own effort. They must show the phase wise development of their project submitting the appropriate documents at the end of each phase.

PROGRAM ELECTIVES

CSE 5233: BIG DATA ANALYTICS [4 0 0 4]

Types of digital data, Introduction to Big Data and Big Data Analytics. Core Hadoop components, Hadoop Ecosystem, YARN and MapReduce, Understanding I/O in MapReduce, Big data serialization formats, Organizing and optimizing data in HDFS, MapReduce with NOSQL as a data source, Applying MapReduce patterns to Big Data, Hive, Pig, Data stream processing with Spark. Introduction to R, RHadoop Architecture, Understanding the Data Analytics Project Life Cycle, Data Analytics Case Studies, Machine Learning with R and Hadoop – Linear Regression, Logistic Regression, Clustering, Recommendation Algorithms, Web Crawling, Inverted Indexes, Baseline Implementation, Inverted Indexing: Revised Implementation, Index Compression, What about Retrieval? Graph Representations, Parallel Breadth first search, PageRank, Issues with graph processing.

References:

1. Seema Acharya and Subhashini Chellappan, *"Big Data and Analytic"s, (1e),* Wiley India Pvt. Ltd., 2015
2. Alex Holmes, "*Hadoop in Practice", (2e),* Manning Publications, 2015
3. Vignesh Prajapati, "*Big Data Analytics with R and Hadoop", (1e),* Packt Publishing, 2013
4. Jimmy Lin and Chris Dyer, "*Data Intensive Text Processing with MapReduce", (1e),* Morgan & Claypool Publishers, 2010
5. Tom White, "*Hadoop: The definitive guide", (4e),* O'reilly, 2015
6. Pramod J Sadalage and Martin Fowler**,** **"***NoSQL Distilled: A Brief Guide to the Emerging World of Polyglot Persistence", (1e),* Addison-Wesley, 2012
7. Paul C Zikopoulos, Chris Eaton, Dirk Deroos, Thomas Deutch and George Lapis, "*Understanding Big Data"*, McGraw-Hill, 2012

CSE 5234 CLOUD COMPUTING [4 0 0 4]

Introduction to Cloud Computing: Reference model, Characteristics, Challenges, Migrating into the Cloud, Cloud Computing Architecture: Infrastructure-as-a-Service (IaaS): Virtualization: Virtualization Technology, role of virtualization in enabling the cloud, applications. Virtual Machines Provisioning and Migration Services, Network virtualization, software defined networking. Platform-as-a-Service (PaaS): Data in cloud: Multithreading& Multitasking programming, Cloud file system, GFS,& HDFS, Map reduce programming model. Software-as-a-Service (SaaS): Service oriented architecture, Understanding web service, Creating cloud based applications. Green computing. Security: Security Concerns and Threats, Access Control, Virtualization Security Management, Cloud Security Risk.

References::

1. Raj Kumar Buyya, Christian Vecchiola and S.Tanurai Selvi ,"*Mastering Cloud Computing*" TMH, 2012.
2. Raj Kumar Buyya, James Broberg and Andrzej Goscinski, " *Cloud Computing Principles and paradigms*", Wiley, 2011
3. Kaittwang Geoffrey C.Fox and Jack J Dongrra, ,"*Distributed and Cloud Computing*" Elsevier India 2012.
4. Gautam Shroff ,"*Enterprise Cloud Computing*", Cambridge University Press, 2012.
5. John Rhoton, "*Cloud Computing Explained*", *(2e)* , Recursive Press, , 2010.
6. Barrie Sosinsky, "*Cloud Computing: Bible",* Wiley India, 2011
7. John W. Rittinghouse and James F. Ransome, "*Cloud Computing, Implementation, Management and Security*", CRC Press, 2010

CSE 5236 DATA MINING AND APPLICATIONS [4 0 0 4]

Data Mining functionalities Major issues in Data Mining, Applications and Trends in Data Mining, Know your data ,attribute types, statistical description of data. Measuring data similarity & dissimilarity measures. Association Rules Mining, Algorithms for discovering frequent itemsets, Advanced pattern mining: Introduction, Pattern mining in multidimensional space , Constraint based frequent pattern mining, Pattern exploration and application, case study. Classification and Prediction , Decision tree induction, Techniques to improve classification accuracy Support vector machines, Classification using frequent patterns , Lazy learners , case study. Clustering Analysis: K-means clustering algorithm, Probabilistic model based clustering , Clustering high dimensional data, Clustering graph and network data case study. Mining data streams, Text mining, Case studies.

Refernces:

1. Jiawei Han, Micheline Kamber,Jian Pei , " *Data mining concepts and Techniques*", *(3e),* Elsevier, 2011
2. Galit Shmueli, Nitin R Patel, Peter C. Bruce, "Data Mining for Business Intelligence", *(2e*), Wiley, 2010 .

3. Sholom M Weiss, Nitin Indurkhya, Tong Zhang, Fred J . Damerau " *Text Mining Predictive methods for analyzing Unstructred Information",* Springer 2005
4. Jiawei Han, Micheline Kamber,Jian Pei , " *Data mining concepts and Tehniques*", *(2e),* Elsevier, 2006
5. T. Davenport, "*Competing on Analytics*," Harvard Business Review (Decision Making), 2006.

CSE 5241 SECURE E-COMMERCE [4 0 0 4]

Early business information interchange efforts, advantages, and disadvantages of E-commerce, E-Business Models. Mechanisms of Classical Money, Instruments of Payment, Types of Dematerialized Monies, Transactional Properties, Practice of Dematerialized Money, Banking Clearance and Settlement. Security of Commercial Transactions, Security objectives, OSI Model, Security Services, Message Confidentiality, Data Integrity, Identification and Authentication of Participants, Access Control, Denial of Service, Nonrepudiation, Management and Exchange of Keys, Kerberos ISAKMP, SKIP, Certificate Management, Encryption Cracks. General Presentation of the SSL Protocol, functional architecture, SSL Sub protocols, Performance Acceleration, Implementations. From SSL to TLS, WTLS: Architecture, Algorithms and Certificate, Messages, Exchange protocol, Location of the WAP/Web Gateway. SET Architecture, Services of SET, dual signature, Certification, Purchasing, Payment Messages, Transaction Progress, Optional Procedures, Implementations, Evaluation. C-SET and Cyber-COMM, Architecture of C-SET, Purchase and Payment, Interoperability, Hybrid SSL/SET Architecture, Transaction Flows, Notification, Settlement, 3-D Secure, Enrolment, Purchase, Payments. Security without Encryption: First Virtual, NetBill, KLELine, Millicent, PayWord, MicroMint, Protection against Forgery, Double Spending, eCoin, Comparison, Second-Generation Systems, Case studies. DigiCash(Ecash), Registration, Loading of Value, Purchase, Delivery, Evaluation, NetCash,, Extensions of NetCash, Evaluation.

References:

1. P.T. Joseph, S.J., "*E-commerce: An Indian Perspective*", *(3e),* PHI, 2009.
2. Mostafa Hashem Sherif, "*Protocols for Secure Electronic Commerce, (2e),* CRC Press, 2005.
3. Anup Gosh, "*E-Commerce Security and Privacy*", Springer, 2001

CSE 5244 WEB SERVICES [4 0 0 4]

Extensible Markup Language (XML), XML Namespaces, Document Type Definitions (DTD) , XML Schema Definition Language (XSD), XML Path Language (XPath), Extensible Stylesheet Language Transformations (XSLT), XML Query Language (XQuery). XHTML and HTML5, Javascript, Asynchronous JavaScript and XML (AJAX), Parsing XML with Document Object Model (DOM). Web Services Definition Language (WSDL), Simple Object Access Protocol (SOAP), Universal Description, Discovery, and Integration (UDDI), Representational State Transfer (REST). Creating and Deploying .NET Web Services, Building a .NET Client to

Consume Web Service. Understanding SOA, Composing Services, SOA Security, SOA Governance. JSON, Resources and Representation, Designing a REST Service, REST vs SOAP, Securing a REST Service. Deploy and Manage API on Amazon Web Services (AWS).

References:

1. Joe Fawcett, Liam R. E. Quin and Danny Ayers, "*Beginning XML", (5e),* Wrox , 2012
2. Leonard Richardson, Mike Amundsen and Sam Ruby, "*RESTful Web APIs", (1e),* O'Reilly, 2013
3. Michael Rosen, "*Applied SOA: Service-Oriented Architecture and Design Strategies", (1e),* Wiley, 2008
4. Christian Nagel, Jay Glynn and Morgan Skinner, "*Professional C# 5.0 and .NET 4.5.1",* Wrox, 2014
5. Ethan Cerami, "*Web Services Essentials, (1e),* O'Reilly, 2002
6. Thomas Erl, "*Service-Oriented Architecture: Concepts, Technology, and Design",(2e),* Prentice Hall, 2016
7. Andreas Wittig, Michael Wittig, "*Amazon Web Services in Action", (1e),* Manning Publications, 2015

CSE 5245 AGENT SYSTEMS AND SECURITY [4 0 0 4]

Intelligent Agents- Introduction, Structure of Intelligent Agents, Environments, Solving Problems by Searching-Problem Solving Agents, Formulating Problems, Searching for Solutions, Search Strategies, Avoiding Repeated States, Constraint Satisfaction Search, Learning from Observations- A General Model of Learning Agents, Inductive Learning, Learning Decision Trees, Security in mobile agent system Problems and approaches Mobile agent security, attacks and countermeasures of software system security, Security issue in a mobile agent system, New formal model, Extended elementary object system (EEOS), Translating the EEOS model to colored petri net model, Simulation and analysis of the extended elementary object system model of a secure mobile agent system, Multiagent Interactions, Reaching Agreements, Working Together, Methodologies.

References:

1. Stuart Russell and Peter Norvig**, "***Artificial Intelligence: A Modern Approach", (3e),* Pearson, 2009.
2. Lu Ma and Jeffrey J P Tsai, "*Security Modeling and Analysis of Mobile Agent Systems",* Imperial College Press, 2006
3. Michael Wooldridge "*An introduction to MultiAgent Systems",* (2e), John Wiley and sons, 2009.
4. Essaaidi, M., Ganzha, M., Paprzycki, M.*, "Software Agents, Agent Systems and their Applications*", IOS Press, 2012.

5. Lin Padgham, Michael Winikoff, "*Developing Intelligent Agent Systems: A Practical Guide*", Wiley, 2004.

CSE 5246 BIOMETRIC SECURITY [4 0 0 4]

Biometrics Fundaments: Introduction, Benefits of biometrics over traditional authentication systems, Benefits of biometrics in identification systems, Selecting a biometric for a system, Applications, Key biometric terms and processes, Verification versus Identification, Logical versus physical access, How biometric matching works, Accuracy in biometric systems. Physiological Biometric Technologies: Fingerprints, Facial scan, Iris and Retina Scan, Hand scan and DNA Biometric Technologies, Technical description, Characteristics, Competing technologies, Strengths and weaknesses, Deployment. Behavioral Biometric Technologies: Handprint Biometrics, DNA Biometrics, Signature and handwriting technology, Technical description , classification, Keyboard /keystroke dynamics, Voice Scan- data acquisition, feature extraction, characteristics, strengths and weaknesses, Deployment. Multi biometrics: Multi biometrics and multi factor biometrics, Two-factor authentication with passwords, tickets and tokens. Applications: Categorizing Biometric Applications, Executive decision, Case studies on Physiological, Behavioral and multifactor biometrics in identification systems.

References:

1. Paul Reid, "*Biometrics for Network Security"*, Pearson Education, 2014.
2. John D. Woodward , "*Biometrics- The Ultimate Reference*", Wiley Dreamtech, 2013
3. John Chirillo and Scott Blaul," *Implementing Biometric Security*", Wiley Publishing Inc., 2013.
4. Ashbourn, J., "*Practical Biometrics - From Aspiration to Implementation*", Springer Verlag, 2004.
5. Anil K. Jain, Patrick Flynn and Arun A. Ross, "*Handbook of Biometrics*" Springer, 2008

CSE 5247 CYBER SECURITY STANDARDS AND BEST PRACTICES [4 0 0 4]

Security problem in computing: definition of secure, Attacks, the meaning of computer security, computer criminals, methods of defense. Administering security: Security planning, Risk analysis, Organizational security policies, Physical security The economics of cyber security: Making a business case, Quantifying security, Modeling cyber security, current research and future directions Privacy in computing: privacy concepts, privacy principles and policies, authentication and privacy, data mining, privacy on the web, e-mail security, impacts on emerging technologies. Legal and ethical issues in computer security: protecting programs and data, information and the law, rights of employees and employers, Redress for software failures, computer crime, Ethical issues in computer security, Case studies of ethics Cyber Security, Hacker Exploits, incident handling Basics, Focus Group, General Drivers of BPs, Cyber security

Best Practices Structure, FGIB cyber security proposals, Survey of current Practices, Creation of new practices, NRIC recovery best practices, NRIC Physical security best practices, Internet of Things, Electronic Voting.

References:

1. Charles P.Pfleegar and Shari Lawrence Pfleeger "Security in Computing" , 5th edition, PHI of India, 2015

2.. John W. Rittinghouse and William N. Hancock "Cyber Security Operations handbook", Elsevier, 2003

CSE 5248 DATABASE AND APPLICATION SECURITY [4 0 0 4]

Introduction to Security, Information Systems, Database management systems, security and Architecture, database security, E- Mail security, Asset types and their value, Security methods, Operating systems overview, security environment, components, Authentication methods, user administration, password policies, Vulnerabilities of operating systems, Defining and using profiles, Designing and implementing password policies, Granting and revoking user privileges, creating, Assigning and revoking user roles.User authentication, operating system authentication, creating/removing/modifying users, default/remote users, Database links, Linked servers, remote servers, know where passwords are maintained, Obfuscate application code, Secure the database from SQL injection attacks, Work toward alignment between the application user model and the database user mode, Types of users, security models, application types, application security models and Data encryption, implementing VPD ,VPD policies and application, Database Auditing Model,Application Data Auditing,DML auction auditing architecture. Triggers, fine grained auditing, Secure database links and watch for link-based elevated privilege, Protect link usernames and passwords, Monitor usage of database links ,Map and secure all data sources and sinks, Auditing Database Activities, project cases, case study for developing an online database, taking care of payroll, tracking database changes and developing a secured authentication repository

References:

1. Hassan A. Afyouni, "*Database Security and Auditing* "India Edition, CENGAGE Learning, 2009.
2. RonBen Natan, "*Implementing Database Security and Auditing*",: Elsevier, Indian reprint, 2006
3. M.TamerÖzsu, Patrick Valdureiz, "*Principles of Distributed Database System"*: Springer , *(3e),* 2011
4. Castano, Fugini, "*Database Security*", Addison Wesley:ACM, 2004
5. Clark, Holloway, List, *"The security Audit and control of Databases",* UK:Ashgate

CSE 5249 INFORMATION SECURITY MANAGEMENT   [4 0   0   4]

Introduction to Information Security: History Of Information Security, Characteristics Of Information, NSTISSC Security Model, Components Of An Information System, Security Systems Development Life Cycle, Security Professional And The Organization, Risk Management: An Overview Of Risk Management, Risk Identification, Identifying Assets, Threats And Vulnerabilities, Risk Control Strategies, Selection A Risk Control Strategy, Risk Analysis And Assessment, Planning For Security, Implementing Information Security, Disaster Recovery And Risk Monitoring, Security Threats To Computer Networks, Computer Network Vulnerabilities, Security Assessment, Analysis, And Assurance: System Security Policy, Building A Security Policy, Security Requirement Specification, Threat Identification, Threat Analysis, Vulnerability Identification And Assessment, Security Monitoring And Auditing

References:

1. Michael E. Whitman and Herbert J. Mattord, *Principles of Information Security, (2e)*, Thomson Learning, 2007
2. NIIT, "*Introduction to Information Security Risk Management"*, PHI, 2004
3. Joseph Migga Kizza , "*A Guide to Computer Network Security"*, Springer-Verlag London Limited, 2010.

CSE 5250 INTRUSION DETECTION SYSTEMS   [4 0   0   4]

Understanding intrusion detection, Intrusion detection and prevention basics, Analysis schemes, IDS and IPS architecture, tired architectures, IDS and IPS internals, defending IDS/IPS, Introduction to Snort, TCP stream follow up, protecting IDS, Installing and working with snort, Installation scenarios, Running Snort on Multiple Network Interfaces , snort Modes , Working with Snort Rules , TCPIP Network layers, The Snort Configuration File , order of Rules Based upon Action , Automatically Updating Snort Rules , CISCO secure IDS, designing your CISCO based solution: Collecting requirements, defense in depth, network IDS, session sniping and shunning, Incident responses, IDS/IPS incident response phases, Extrusion Detection, defining the Security Process, Security Principles, Network Security Monitoring Theory and Tools, Defensible network architecture, Extrusion detection through NSM. Policy and procedures, Creating an IDS/IPS policy, legal review, Future of Intrusion detection and prevention, Lower reliance on signature based intrusion detection, integrated forensic capabilities.

References:

1. Endorf, C., Schultz E. and Mellander J,"*Intrusion Detection and Prevention",(2e)* McGraw-Hill, 2006.
2. Richard Bejtlich "*Extrusion detection-Security Monitoring for Internal Intrusions",(1e),* Addison Wesley, 2006

3. Rafeeq Rehman “ *Intrusion Detection with SNORT, Advanced IDS techniques using Snort, Apache, MySQL, PHP and ACID*”, *(1e),* Prentice Hall , 2003
4. Rash, M., Orebaugh, A. and Clark, G., “*Intrusion Prevention and Active Response: Deploying Network and Host IPS*”, *(2e),* Syngress,USA, 2005.
5. Rebecca Gurley Bace, “*Intrusion Detection*”, *(2e),* Macmillan Technical Publishing , 2000

CSE 5251 LEGAL ISSUES IN INFORMATION SECURITY [4 0 0 4]

Introduction to Information Security-The History of Information Security, What Is Security? Key Information Security Concepts,Critical Characteristics of Information,CNSS Security Model, Components of an Information System, Balancing Information Security and Access,Approaches to Information Security Implementation, The Systems Development Life Cycle,The Security Systems Development Life Cycle ,Security Professionals and the Organization, Information Security Project Team, Communities of Interest, Case. The Need for Security-Business Needs, Types of Threats, Types of Attacks, Secure Software Development, Case Exercises, Legal, Ethical, and Professional Issues in Information Security-The Information Technology Act, 2000(No. 21 OF 2000)- The Patents Act 1970(incorporating all amendments and rules-till 2015)-Copy Right Act 1957(incorporating all amendments and rules-till 2015) Planning for Security-Introduction, Information Security Planning and Governance, Information Security Policy, Standards, and Practices, The Information Security Blueprint, Security Education, Training, and Awareness Program, Continuity Strategies. Information Security Maintenance- Introduction, Security Management Maintenance Models, Digital Forensics.

References:

1. RasoolAzari, “*Current Security Management & Ethical Issues of Information Technology*” Idea Group Publishing, 2003
2. Alexander I., Poltorak Paul, J. Lerner “*ESSENTIALS of Licensing Intellectual Property*”, John Wiley & Sons, Inc.
3. John R. Vacca,*“Computer Crime Scene Investigation”,(2e),* Charles River Media, an imprint of Thomson Learning Inc., 2005.
4. Lech J. Andrew M. Colarik, *“Cyber Warfare and Cyber Terrorism*”, IGI Global 2007.
5. Michael Erbschloe “*Information Warfare How to Survive Cyber Attacks*”, Osborne/McGraw-Hill, 2001

CSE 5252 MOBILE AND WIRELESS SECURITY [4 0 0 4]

Introduction to Security and Privacy for Mobile and Wireless Networks, Pervasive Systems, Mobile system architectures and Security & Attacks, Wireless security, Scanning and Enumerating 802.11 Networks, Attacking 802.11 Networks, Attacking WPA protected

802.11 Networks, Bluetooth Scanning and Reconnaissance, Bluetooth Eavesdropping, Attacking and Exploiting Bluetooth, ZigBee Security, ZigBee Attacks, Security in Ad Hoc Wireless Networks, Motivations and application fields, Routing protocols, Key Management in Adhoc Wireless Networks, Group key management within ad hoc networks, Radio Frequency Identification (RFID), RFID an anti-counterfeiting tool, Enhance Privacy in RFID Systems, An Efficient and Secure RFID Security Method with Ownership Transfer, Scalability Issues in Large-Scale Applications, Dynamic Privacy Protection for Mobile RFID Service, Security in next generation mobile networks and wireless sensor network, IP Multimedia Subsystem (IMS), 4G security, Confidentiality, Attacks on wireless sensor networks and counter-measures, Prevention mechanisms: authentication and traffic protection.

References:

1. Kia Makki, Peter Reiher, "*Mobile and Wireless Network Security and Privacy"*, Springer, 2007.
2. Noureddine Boudriga, "*Security of Mobile Communications"*, CRC Press, 2009.
3. Kitsos Paris, Zhang Yan, "*RFID ecurity Techniques, Protocols and System-On-Chip Design"*, Springer, 2008.
4. Johny Cache, Joshua Wright and Vincent Liu, "*Hacking Wireless Exposed: Wireless Security Secrets & Solutions*," *(3e*), McGraw-Hill Osborne, 2015.
5. Hakima Chaouchi, Maryline Laurent-Maknavicius, "*Wireless and Mobile Network Security"*, Wiley-ISTE, 2009.

CSE 5253 OBJECT ORIENTED SYSTEM DESIGN [3 0 2 4]

The World of the Modern Systems Analyst, Object Oriented Development and the Unified Process, Project Management and the Inception Phase, The Requirements Discipline, Use Cases and Domain Classes, Use case modelling and detailed requirements, Design activities and Environments, Use Case Realization: The Design Discipline within Unified Process Iterations, Advanced Topics in Object Oriented Design, Designing the Data Access Layer, Designing the User Interface Layer, Designing System Interfaces, Controls and Security , Software Quality Assurance, System Usability and Measuring User Satisfaction.

References:

1. Satzinger, Jackson, Burd, "*Object-Oriented Analysis and Design With the unified Process"*, Thomson,2007.
2.Ali Bahrami, "*Object Oriented Systems Development*", Tata McGraw-Hill, 2012.
3.James Rumbaugh, Ivar Jacobson, Grady Booch "*The Unified Modeling Language Reference Manual*", Addison Wesley, 1999.
4. Tom Pender "*UML Bible*", Wiley, 2003.

5. UML 2.0 Superstructure - Final Adopted Specification. Object Management Group, 2003 http://www.omg.org/docs/ad/03-08-02.pdf.

CSE 5254 PUBLIC KEY INFRASTRUCTURE (PKI) AND TRUST MANAGEMENT [4 0 0 4]

Introduction, The Concept of Public Key Infrastructure, PKI services, Trust Models -Strict and Loose Hierarchy of Certification Authorities, Policy-Based Hierarchies, Distributed Trust Architecture, Four-Corner Trust Model Web Model, User-Centric Trust, PKI Data structures, Cross-Certification, Entity Naming, Certificate Path Processing, PKI interoperability; PKI-Enabled Services, Secure communication, secure time stamping, Notarization, Non-repudiation, Privilege Management, Mechanisms Required to create PKI Architecture, Access Control Mechanisms, PKI-Enabled Services, Operational Considerations; Certificates and Certification, Certificates, Certificate Policies, Certificate Authority, Registration Authority; PKI Information Dissemination-Private Dissemination, Publication and Repositories, Interdomain Repository Issues and Options, In-band Protocol Exchange; PKI Operational Considerations- Client-Side Software, Off-line Operations, Physical Security, Hardware Components, User Key Compromise, Disaster Preparation and Recovery;Electronic Signature Legislation and Considerations; Major Standards and PKI Interoperability- X.509, PKIX, X.500, LDAP, ISO TC68, ANSI X9F, S/MIME, IPsec, TLS, SPKI, OpenPGP EDIFACT, IEEE, WAP, XML-Based Activities, Other Activities; Deployment Considerations-Draft a certificate policy, Establishing policy mappings and constraints, Local certificate and CRL profiles, Select a PKI product or Service provider, Certification Practice Statement, Critical Deployment issues, Apply for a Licenses Certification Authority, PKI Deployment case studies. PKI Operation Risks Verifying identity, Certificate content, Certificate creation, Distribution, and Acceptance, Internal security concerns, Managing Digital Certificates.

References:

1. Carlisle Adams, Steve Lloyd, "*Understanding PKI: Concepts, Standards, and Deployment Considerations*", *(2e),* Addison Wesley, 2003

2. Suranjan Choudhary "*Public Key Infrastructure Implementation and design*" M&T books, 2002

3. David F. Ferraiolo "*Role-Based Access Control*", *(2e),,* Artech house, 2006

4. Request For Comments- RFC2510, RFC 2559, RFC 3280, RFC 3379, RFC 3647, RFC 4158, RFC 4476 etc

5. Ashutosh Saxena, "*Public Key Infrastructure- Concepts, Design and Deployment*", TMH, 2003

OPEN ELECTIVES

CSE 5281 INFORMATION STORAGE AND MANAGEMENT [3 0 0 3]

Introduction to Information Storage and Management, Evolution of Storage Technology and Architecture, Data Center Infrastructure, Data Protection, RAID, RAID Components, RAID Levels, RAID Impact on Disk Performance, Hot Spares, Intelligent Storage systems, EMC Symmetrix, Direct Attached Storage, Storage Area Networks, FC Connectivity, Fabric Ports, World Wide Names, Zoning, Fabric Login Types, FC Topologies, Network Attached Storage, Components, Benefits and Implementations of NAS, NAS File-Sharing Protocols, Content-Addressed Storage, Fixed Content and Archives, CAS Architecture, Object Storage and Retrieval in CAS, Backup and Recovery, Backup Purpose, Backup Considerations, Backup Granularity, Recovery Considerations, Backup Methods, Backup Process, Backup and Restore Operations, Local Replication, Remote Replication.

References:

1. G. Somasundaram, Alok Shrivastava, "*Information Storage and Management-Storing, Managing, and Protecting Digital Information in classic, virtualized and cloud environments", (2e)*, EMC Education Services, John Wiley & Sons Inc., 2012.
2. G. Somasundaram, Alok Shrivastava, *"Information Storage and Management-Storing, Managing, and Protecting Digital Information"*, EMC Education Services, Wiley Publishing Inc, 2009.
3. Marc Farley, "*Storage Networking Fundamentals", (1e),* CISCO Systems, 2004.
4. Robert Spalding, "*Storage Networks: The Complete Reference"*, Tata Mcgraw Hill, 2003.
5. Marc Farley Osborne, "*Building Storage Networks", (2e)*, Tata McGraw Hill, 2001.

CSE 5282 MULTICORE PROGRAM OPTIMIZATION [3 0 0 3]

Introduction to parallel computers; Instruction Level Parallelism (ILP); Data parallelism; Multiprocessors and thread level parallelism; Shared Memory Multiprocessors; Cache coherence problems; Snoopy protocols; Memory consistency models; Hyper threading technology architecture; multi-core architecture; Multi-threading on single core versus multi-core platforms; Amdahl's law; Power consumption; Introduction to Basic optimization; Hot Spot, Faster Algorithms, Data Dependency, Branching, Memory, Loops, Slow Operations; Introduction to

Performance Tools (Intel Software Tools); Introduction to Multi-core Optimization; ILP vs TLP, Data vs Task Parallelism, Threading and Parallel programming constructs, Threading APIs, Multi Threading with OpenMP, Threading Goals and Issues; Multithreaded and Parallel Applications Case studies; Some applications in Integer Programming, Digital Signal Processing(Video Codec)

References:

1. Richard Gerber, Aart J. C Bik, Kevin B. Smith, and Xinmin Tian, "*The Software Optimization Cookbook High Performance Recipes for IA-32 Platforms"*, *(2e)*, Intel Press, 2006
2. Shameem Akhter, Jason Roberts, "*Multi-Core Programming: Increasing Performance through Software Multi-threading"*, Intel Press, 2006
3. J. L. Hennessy and D. A. Patterson, "*Computer Architecture: A Quantitative Approach", (5e),* Morgan Kaufmann Publishers, 2014
4. D. E. Culler, J. P. Singh, A. Gupta, "*Parallel Computer Architecture: A Hardware/Software Approach"*, Morgan Kaufmann Publishers, 2nd Edition, 1997
5. Darry Gove, "*Multicore Application Programming for Windows, Linux and Oracle Solaris"*, Addison-Wesley, 2011
6. Barbara Chapman, Gabriele Jost, Ruud Van Der Pas, "*Using OpenMP portable shared memory parallel programming"*, The MIT Press, 2008