Master of Technology in Computer Science & Engineering with Specialization in Information Security

Program Outcomes:

PO1. To prepare trained manpower needed for academics, research and development of information and communication technologies for industries and research organization related to the field.

PO2. To understand and follow the process of research leading to a thesis with innovative contribution leading to addition of knowledge to the existing body of the state of the art.

PO3. To sensitize and train young students as future researchers in the frontier areas of information security and allied areas.

PO4. To train students to understand theoretical aspects of computing and cyber security with understanding of security requirements of a system, software or organization.

PO5. To deliver the understanding of practical implementations of security mechanisms, analyzing deployed security mechanisms with computational and economic aspects.

PO6. To prepare trained individuals to tackle emerging research and engineering issues in computing domain in general and also with a focused approach on information security domain.

PO7. To train students with a thorough practical knowledge and problems solving skills to approach newer technological problems in the security domain and computing domain in general.

Program Specific Outcomes:

1. At the end of the program, graduates will be able to get insights into various fields of information security with a deep understanding of theoretical aspects of security and related analysis.

2. Graduates should also get a broader understanding of various security systems, protocols, complexities, standards, practical applicability, and their limitations.

3. During the course, students should enhance their inquisitiveness to ever-evolving domain of information security and apply their knowledge to solve problems.

4. With a focused one year research leading to a thesis, students should be able to understand the "art" and "science" of research and should be capable enough to apply this training to newer/other fields and problems.

5. Students should also be able to solve security issues with understanding of system security and cryptographic attributes with a relevance to standards

Mapping of COs of core courses and POs

Sr. No.	Title of the course	Course Code	PO1	PO2	PO3	PO4	PO5	PO6	PO7
1	Probability Theory and Distributions	CSE601	✓	✓	●	✓	●	●	●
2	Algorithm and Complexity	CSE602	✓	✓	✓	✓	●	✓	●
3	Advance Computer Systems	CSE603	✓	✓	✓	●	✓	✓	✓
4	System Design Lab	CSE604	✓	●	✓	●	✓	✓	✓
5	Machine Learning	CSE610	✓	✓	●	●	✓	✓	✓
6	Cryptography and Network Security	CSE611	✓	✓	✓	✓	✓	●	✓
7	Number Theory	CSE612	✓	●	✓	✓	●	✓	✓
8	Security Engineering	CSE615	✓	✓	✓	●	✓	✓	✓
9	Dissertation – I	CSE616	✓	✓	✓	✓	✓	✓	✓
10	Dissertation – II	CSE620	✓	✓	✓	✓	✓	✓	✓

Scheme and Detail Syllabus

M.Tech. Computer Science & Engineering

(Specialization in Information Security)

First Year

SEMESTER I						
Sr. No	**Course Code**	**Course Name**	**L**	**T**	**P**	**Credits**
			Hours/week			
1	CSE601	Probability Theory and Distributions	3	1	0	4
2	CSE602	Algorithm and Complexity	3	0	2	4
3	CSE603	Advance Computer Systems	3	0	2	4
4	CSE604	System Design Lab	3	0	2	4
5		Program Elective– I	3	0	2	4
6	CSE681	AECC1	0	2	0	2
Total Credits						**22**

SEMESTER II						
Sr. No	**Course Code**	**Course Name**	**L**	**T**	**P**	**Credits**
			Hours/week			
1	CSE610	Machine Learning	3	0	2	4
2	CSE611	Cryptography and Network Security	3	0	2	4
3	CSE612	Number Theory	3	0	2	4
4		Program Elective – II	3	0	2	4
5		Open Elective – I	3	0	2	4
6	CSE682	AECC2	0	2	0	2
Total Credits						**22**

Second Year

SEMESTER III						
Sr. No	**Course Code**	**Course Name**	**L**	**T**	**P**	**Credits**
			Hours/week			
1	CSE615	Security Engineering	3	0	2	4
2		Program Elective – III	3	0	2	4
3	CSE616	Dissertation – I	0	0	14	14
Total Credits						**22**

SEMESTER IV						
Sr. No	**Course Code**	**Course Name**	**L**	**T**	**P**	**Credits**
			Hours/week			
1	CSE620	Dissertation – II	0	0	22	22
Total Credits						**22**

Proposed Courses under AECC having 2 credit each in each semester

1. IT Tools
2. Professional Communication
3. Programing Language
4. Use of ICT Application

Note: The students may opt to take Elective courses through SWAYAM portal as approved by the department.

List of Electives (Program / Open Elective)

Following list has to be used for offering ProgrammeElective/ Open Elective. Additional Elective can be added as and when required after taking departmental approval.

Course Code	Programme / Open Elective (s)
CSE631	Quantum Cryptography
CSE632	Information Security Audit and Assurance
CSE633	Security Analysis of Protocols
CSE634	Cyber Crime, Forensics and Information Warfare
CSE635	Public Key Infrastructure and Trust Management
CSE636	Digital Watermarking and Steganalysis
CSE637	Data Mining and Machine Learning
CSE638	Simulation and Modeling
CSE639	Optimization Techniques
CSE640	Topics in Operating Systems
CSE641	Topics in Computer Architecture
CSE642	Advanced Compiler Design
CSE643	Advanced Topics in Databases
CSE644	Mobile Computing
CSE645	Advance Software Engineering
CSE646	Multimedia System and Security
CSE647	Secure Programming Techniques
CSE648	Network Protocols
CSE649	Cloud Computing
CSE650	Parallel Processing
CSE651	Digital Image Processing
CSE652	Biometrics and Security
	More to be added

Detailed Structure of the Programme

SEMESTER I: M.Tech (Computer Science and Engineering) with specialization in Information Security

CSE601: Probability Theory and Distributions

Course Objectives:

1. To provide students with a formal treatment of probability theory.
2. To equip students with essential tools for statistical analyses.
3. To foster understanding through real-world statistical applications.

Course Outcomes:

At the end of the course students should be able to:

1. Develop problem-solving techniques needed to accurately calculate probabilities.
2. Apply problem-solving techniques to solving real-world events.
3. Apply selected probability distributions to solve problems.
4. Present the analysis of derived statistics to all audiences.

Course Outlines:

Probability Theorem: Properties of probability, Conditional probability, Independence, Bayes theorem.

Discrete Distributions: Probability distribution functions and cumulative distribution functions.

Continuous Distributions: Probability density functions and cumulative distribution functions, joint and marginal probability density functions.

Mean and variance; moment -generating functions, Marginal and conditional probability distributions, some specific discrete distributions.

Functions of Random Variables: Distribution function technique, Transformation technique, Moment-generating function techniques.

Text/References:

1. DeGroot, Morris H., and Mark J. Schervish. Probability and Statistics. Addison-Wesley.
2. Feller, William. An Introduction to Probability Theory and Its Applications, Wiley.
3. Freund, W.J., Mathematical Statistics, Prentice-Hall.
4. Hoel, P.G., Mathematical Statistics, John Wiley & Sons.
5. Hogg, R.V., & Craig, A.T., Introduction to Mathematical Statistics, Prentice-Hall, Inc.
6. Mood, A.M., Graybill, F.A., Boes, D.C., Introduction to the Theory of Statistics, McGraw Hill.
7. Papoulis: Probability, Random Variables and Stochastic Processes, McGraw Hill.

CSE202: Algorithms and Complexity

Course Outlines: The course focuses on advanced topics in algorithms like B-Trees, Fibonacci heaps, amortized analysis, graph algorithms, randomized algorithms, approximation algorithms, Theory of NP-Hard and NP-Complete Problems.

Course objectives:
The course is designed to train the graduates:

1. To understand the proof of correctness and running time of the algorithms for the classic problems in various domains.
2. To be able to know the concepts of the algorithms and to know the efficiency of the algorithms.
3. To be enable to formalize with theoretical computer algorithms.
4. To apply algorithmic design paradigms and methods of analysis and hence synthesize efficient algorithms in common engineering design situations.

Course Outcomes:
Graduates after completing the course shall gain:

1. Ability to apply the algorithms and design techniques to solve problems.
2. Ability to develop concepts, logics towards solving an unknown problem in IT and research.
3. Ability to explain what competitive analysis is and to which situations it applies in order to perform competitive analysis.
4. Ability to get formalizes theoretical concepts of computer algorithms.

Course Contents

Advanced Data Structures: Brief overview of Notations and Recurrence analysis, Amortized analysis, B- Trees, AVL trees, Dictionaries and tries, Binomial Heaps, Fibonacci Heaps, Disjoint Sets, Union by Rank and Path Compression.

Graph Algorithms: Topological sorting, Articulation point, All-PairsShortest Paths, Spanning Tree, Maximum Flow and Bipartite Matching.

Randomized Algorithms and Approximation algorithms: Finger Printing, Pattern Matching, Graph Problems,Algebraic Methods, Probabilistic Primality Testing. Polynomial Time Approximation Schemes, PTAS, FPTAS, Approximation algorithms for vertex cover, set cover, TSP problem etc.

Theory of NP- Hard and NP-Complete Problems: Definitions of P, NP, NP-Hard and NP-Complete Problems, Optimization and Decision Problems, Reducibility, Cook's Theorem, Satisfiability problem, NP completeness reductions examples.

Text/References:

1. T. H. Cormen, C. E. Leiserson, R. L. Rivest, Introduction to Algorithms, Prentice Hall.
2. Aho, Hopcraft, Ullman, Design and Analysis of Computer Algorithms, Addison Wesley.
3. R. Motwani and P. Raghavan Randomized Algorithms, Cambrdige University Press.
4. C. H. Papadimitriou, Computational Complexity, Addison Wesley.
5. S. Basse, Computer Algorithms: Introduction to Design and Analysis, Addison Wesley.

CSE603: Advanced Computer Systems

Course Outline: This is an advanced course which focuses on advance topics such as network design and operating systems, performance issues and implementation issues in modern enterprises. In addition, this course also targets to give an overview of various modern forms of networks such as sensor networks, vehicular networks, under-water and body area networks.
Prerequisites: An undergraduate level course on computer networks.

Course objectives:

1. This course aims at delivering concepts related to introduction to networking components, their hardware, software stack and their implementation.
2. In addition, this course targets at discussing concepts related to network performance, evaluation, simulation at length with limitations of various techniques.
3. It also focuses on advanced concepts in Operating Systems. Inter Process Communication shall be studied in detail.
4. This course also focus on providing an overview of newer forms of computer networks such as sensor networks, vehicular networks, underwater and body area networks and their related protocols, performance issues and suitable usage with case-studies.
5. This course also aims at taking cases of enterprises for possible network design with respect to scale, applications, performance and capacity planning.

Course Outcomes:

1. At the end of this course students should be able to understand the TCP/IP software stack and its relation with layered architecture in the code.
2. In addition, students should be able to understand various network protocols, their open-source implementations, performance issues, and simulations.
3. Understanding various newer forms of networks with their features, limitations and related protocols.
4. Participants of this course should be able to understand cases of enterprises/organizations and should be able to design network diagram, capacity planning and addressing and devices needs.
5. Participants of this course should be able to implement ipc in real time systems

Course Contents:

Introduction: Introduction to Layered architecture, Networking hardware and softwarestacks.
Network Performance: Network Simulation and Modeling, Performance issues in networks, Protocol case studies (e.g. HTTP, HTTPS, SSL, DHCP, DNS, Transport protocols and Routing protocols in wired and wireless networks and their performance).
Modern Networks: Mobile Networks, Sensor Networks, Vehicular Networks,Underwater Networks and Body Area networks and related performance issues.
Enterprise networks: Enterprise network infrastructure planning and design. Capacityplanning of servers and data centers.
Inter Process Communications:concepts of IPC, Pipes, FIFOS, Message queues, Semaphores, Sockets API,

Text/ References

1. Selected research papers for most of the topics.
2. Top-Down Network Design- Networking Technology, Author Priscilla Oppenheimer, Publisher- Pearson Education, 2010.
3. Computer Networking: A Top-Down Approach (6th Edition), J Kurose and KW Ross, Pearson, 2012.

CSE604: System Design Lab

Course Outline: This course is a lab-oriented course with a focus on learning system design principles and applying them while implementing possible systems with practical functionalities. In addition, a strong focus on secure coding principles is required to cater to the needs of information security discipline.

Prerequisites: A course on programming or software engineering

Course objectives:

1. This course aims at teaching practical aspects of system design with an explicit focus on security as a property of the systems and not as a feature.
2. The course aims at delivering various practical concepts related to secure design life cycle with additional important concepts such as coding guidelines, secure code development, risk analysis, threat modeling, defensive coding and related concepts.
3. With the help of tutorials, lab sessions and course projects, students should understand the practical ideas related to cryptography and related APIs, deployment and distribution, Insider Threat, Case studies, Common Vulnerability Scoring System, and Usability aspects in secure software design.

Course Outcomes:

1. Being a practical, lab and project driven course, students should be able to understand the security needs and related implementation of any systems which would have been otherwise analyzed and designed without security in mind using software engineering principles.
2. Participants of this course should be able to understand the need and uses of defensive and secure programming techniques with risks and threats in mind.
3. Student should also be able to learn and implement concepts related to at least one practical crypto APIs.

Course Contents:

UNIT 1: Software Design Life Cycle models and role of security. Secure Design and Coding Principles and Policies.

UNIT 1: Misuse and Abuse Cases, Risk Assessment, Test Planning, Threat Modeling, Distrustful Decomposition, Defensive Coding, Validation and Sanitization.

UNIT 3: Code Inspection, Code Coverage, Permissions, Access Control, Crypto APIs and use of safe APIs

UNIT 4: Deployment and Distribution, Insider Threats: Cases and Solutions, CVSS, Usability and Accessibility Aspects.

Program Elective – I	Any course from list of elective

SEMESTER II: M.Tech (Computer Science and Engineering) with specialization in Information Security

CSE610: Machine Learning

Course Objectives:

1. Introduce the fundamentals of machine learning.
2. Provide understanding of techniques, mathematical concepts, and algorithms used in machine learning.
3. Provide understanding of the limitations of various machine learning algorithms and the way to evaluate performance of machine learning algorithms.

Course Outcomes:

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

1. Understand the basic concepts of machine learning.
2. Identify the suitable machine learning algorithm to solve a machine learning problem.
3. Analyze the performance of machine learning models.
4. Structuring machine leaning and deep learning projects
5. Develop real-time applications based on machine/deep learning.

Course Contents:

Introduction: Machine learning, types of machine learning, applications of machine learning systems, designing a learning system, the concept learning, concept of hypotheses, version spaces and the candidate elimination algorithm.

Regression: Correlation, causation, simple linear regression, multiple linear Regressions, loss functions: mean squared error, mean absolute error, cross entropy, regression tree.

Classification and Clustering: Decision tree classification, Naïve Bayes classification, K-Nearest Neighbor Classification, logistic regression: binary classification, multiclass classification, K-Means Clustering.

Artificial Neural Networks: Biological motivation, neural network representation, perceptrons, optimization algorithm, Introduction to deep learning, implementation of deep ANN multi-class classification, hyper-parameters tuning, convolution neural network (CNN).

Text/References:

1. Bishop, C. (2006) Mitchell, T. M. (1997) Machine Learning. McGraw-Hill
2. Pattern Recognition and Machine Learning. Berlin: Springer-Verlag.
3. Recent Research Papers.

CSE611: Cryptography and Network Security

Course objectives:

The course is designed to train the graduates in:

1. In depth understanding of network security.
2. In depth understanding of the Cryptographic Techniques.
3. To apply cryptographic techniques in computer systems.
4. To design new or modify existing cryptographic techniques.
5. To work in research institutions / Industry in the field of Security.

Course Outcomes:

Graduates after completing the course shall gain:

1. Ability to understand concepts of network security and cryptographic techniques.
2. Ability to design and analyze cryptographic techniques.
3. Ability to solve network security issues in real time applications.
4. Ability to take up doctoral level research work in security.

Course Contents:

Cryptography: Introduction, steganography, Public versus private key cryptography.

Stream Ciphers: Conventional Ciphers, play fair, Hill, mono-alphabetic and poly-alphabetic.

Private-key cryptography: Feistel structure, DES, design of S-boxes, AES, Triple DES, Differential and linear cryptanalysis.

Public key cryptography: Key management, Diffie-Hellman,ElGamal, RSA. Random Number Generation, Primality testing, Elliptic Curves and ECC.

Digital Signature: DSA and its variants, discrete logarithm based digital signatures.

Network Security: Authentication and signature protocols; Kerberos, real-time communication security, IPsec: AH, ESP, IKE; SSL/TLS, e-mail security, PEM and S/MIME, PGP, web security, network management security, wireless security. Threats in networks, firewalls, intrusion detection, Honeypots, password management.

Text/References:

1. D.R. Stinson, Cryptography - Theory and practice, CRC Press.
2. A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, Applied Cryptography, CRC Press.
3. Stallings, Cryptography and Network Security, Pearson Education.
4. B Schneider, Applied Cryptography, Wiley. ISBN 0-471-11709-9
5. C. Kaufman, R. Perlman, Network Security, Prentice Hall.
6. https://nptel.ac.in/courses/106105162/
7. https://nptel.ac.in/courses/106105031/13

Number Theory(CSE612)

Course objectives:
The course is designed to train the graduates:
1. To understand the use of pure mathematics in coding theory, cryptology, and computer science.
2. To be able to get logical thinking, and the ability for symbolic manipulation in order to understand the sophisticated mathematical tools.
3. To get knowledge of exercise sets containing thought-provoking true/false problems, numeric problems and various proof techniques to develop computational skills.

Course Outcomes:
Graduates after completing the course shall gain:

1. Ability to emphasis on problem-solving techniques such as doing experiments, collecting data, recognizing patterns, and numeric computations exercises.
2. Ability to understand the thought-provoking applications spread throughout, establishing a strong and meaningful bridge with geometry, computer science.
3. Enable to develop the problem-solving skills, hands-on experience with concepts and enhance the opportunity for computational exploration and experimentation.

Course Outline:

Number Systems: Natural numbers, Mathematical induction, Recurrence relations, The Division Algorithm, Catalan Numbers, Prime and Composite Numbers, Fibonacci and Fermat Numbers Greatest Common Divisor, Euclidean algorithm, Fundamental theorem of Arithmetic.
Diophantine equations: Modulo arithmetic, Congruence classes, Modular Exponentiation, Towers of Powers Modulo m, Linear Congruences, Multiplicative inverse, Systems of Linear Congruences, Chinese remainder theorem, Wilson's Theorem, Euler's extended algorithm, Fermat's little theorem, Multiplicative Functions, Totient function, Euler's theorem.
Elementary number theory: Prime numbers, Number bases, Primality testing algorithm, Primitive Roots and Indices, The Order of a Positive Integer, discrete logarithm, primitive roots for Primes, Number sieves, The Algebra of Indices, Quadratic Residues, The Legendre Symbol.
Text/References:
1. Thomas Koshy, Elementary Number Theory with applications, Elsevier India, 2005.
2. Menezes, A, et.al. Handbook of Applied Cryptography, CRC Press, 1996
3. D.R. Stinson, Cryptography - Theory and practice, CRC Press.
4. Koblitz, N. Course on Number Theory and Cryptography, Springer Verlag, 1986
5. Martin Erickson and Anthony Vazzana: Introduction to Number Theory, Chapman &Hall/CRC.

Program Elective – II	Any course from list of elective

Open Elective – I	For details, refer to the concerned department offering t course.

SEMESTER III: M.Tech (Computer Science and Engineering) with specialization in Information Security

CSE615: Security Engineering

Course Outline: This course on security engineering focuses on providing concepts related to buildingsecure systems including secure software, hardware and development and evaluation of such systems.

Prerequisites: Courses on Operating Systems, Computer Networks, Programming, Security and Cryptography

Course Objectives:

1. This course aims to deliver concepts related to building secure systems. This include discussion related to building system using passwords, biometrics, CAPTCHA's, secure programming techniques, trusted computing, Crypto APIs and physical security.
2. This course also aims at equipping students with a variety of security attacks, their sophistication, and defense mechanisms.
3. This course also aims at discussing various cases of security attacks, losses, and possible revival against such attacks utilizing state of the art.

Course Outcomes:

1. At the end of this course, students should be able to understand various concepts related to engineering secure systems by keeping various threats in mind.
2. Understanding of principles related to use of authentication mechanism, their form, security analysis, overhead, use of security standards related to cryptography and physical security.

Course Contents:

Introduction to Security Engineering: Passwords and their limitations, attacks on passwords, CAPTCHA, Biometrics.
Access Control: ACL, sandboxing, virtualization, trusted computing. Multi-level and Multi-lateral security.
Securing services: Security in Metered Services, pre-payment meters. Secure printing and Seals. Tamper resistance mechanisms.
Secure systems: hardware, software and communication systems – design issues and analysis.
Secure software architecture: models and principles, hardware design related security – smart cards and other security solutions, communication protocols and application systems associated with security.
Attacks and defenses: Phishing, social networking attacks, Denial of service, API attacks, network attacks and countermeasures, side-channel attack, advanced persistent Threats (APTs)
Copyright and DRM.

Text/References:

1. Ross J. Anderson: Security Engineering: A Guide to Building Dependable Distributed System. Wiley.
2. Selected papers and online material.

CSE616: Dissertation – I

This is the first part of the major dissertation wherein every student shall be expected to contribute to domain knowledge incrementally. It is expected that the work should be focused in a particular area for concept, design, implementation and analysis. For this first part, assessment shall be done by the external examiner through an open seminar with a feedback to department chair.

Program Elective – III	Any course from list of elective

SEMESTER IV: M.Tech (Computer Science and Engineering) withspecialization in Information Security

CSE620: Dissertation – II

This will be culmination of dissertation – I of semester – III. In this Stage-II the evaluation shall be done through an Open seminar with an external examiner. Thesis shall be submitted with abstract. The school should work to standardize the thesis template for uniform submissions.

Electives

1. Quantum Cryptography(CSE631)

Course objectives:

The course is designed to train the graduates in:

1. In depth understanding of quantum cryptography.
2. Understanding of the cryptographic techniques.
3. To understand quantum cryptography encryption and decryption schemes.

Course Outcomes:

Graduates after completing the course shall gain:

1. Ability to understand concepts of quantum cryptography and cryptographic techniques.
2. To work in research institutions / Industry in the field of quantum cryptography.
3. To design new or modify existing quantum cryptographic techniques.

Course Contents:

Finite Dimensional Hilbert Spaces – Tensor Products and Operators on Hilbert Space – Hermitian and Trace Operators - Basic Quantum Mechanics necessary for the course.
Quantum Gates and operators and Measurement – Quantum Computational Model – Quantum Complexity – Schemes for Physical realization (Only peripheral treatment expected).

Shor's Algorithm – Application to Integer Factorization – Grover's Algorithm.
Quantum Cryptography: Encryption and decryption schemes.

Text/References:

1. Nielsen M. A. and I. L. Chauang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2002.
2. J. Gruska, *Quantum Computing*, McGraw Hill, 1999.
3. P. R. Halmos, *Finite Dimensional Vector Spaces*, Van Nostrand, 1958.
4. Selected papers and online material.

2. Information Security Audit and Assurance(CSE632)

Course Outline: This course focuses on concepts related to audit and assurance mechanisms related to information security mechanisms such as security policies, their enforcement through software, authentication, cryptography and physical security and their progression through the course of time.

Prerequisites: Course on information security.

Course Objectives:

1. Participants of this course should be able to understand the audit procedures related to systems and related software in general in addition to hardware components.
2. In addition, formation of security policies related to various services, components, devices, physical location and acceptable use policies.
3. This course also aims at learning auditing standards and their requirements both from technical and legal perspectives.

Course Outcomes:

1. Students should be able understand the need and methods of writing un-ambiguous, usable, and precise security policies.
2. During this course, students should be able to understand the need of audit procedures, methods of auditing, auditing standards, importance of language in security policies and technical difficulties and circumvention mechanisms while implementing such policies.
3. Audit and assurance during software design lifecycle and concurrent auditing.

Course Contents:

Security policies, policy languages, confidentiality policies, Bell-LaPadula model, controversies over the model.
Integrity policies, Biba model, Lipner's model, Clark-Wilson models, Chinese wall model, clinical information systems security policy, noninterference and policy composition. Assurance and trust, building secure and trusted systems, waterfall model, other models of development.
Assurance in requirements definition and analysis, assurance during system and software design, assurance during implementation and integration.

Information Security Audit and Auditory standards.

Text/References:

1. M. Bishop, Computer Security: Art and Science, Pearson Education, 2003.
2. W. Mao, Modern Cryptography: Theory & Practice, Pearson Education, 2004.
3. C. P. Fleeger and S. L. Fleeger, Security in Computing, 3/e, Pearson Education, 2003.

3. Security Analysis of Protocols(CSE633)

Course objectives:

The course is designed to train the graduates in:

1. Introduce concepts of Security Analysis.
2. In depth understanding of security analysis both Formal and Automated.
3. Designing and analyzing the security of Security Protocols.
4. To work in research institutions / Industry in the field of Security.

Course Outcomes:

Graduates after completing the course shall gain:

1. Ability to understand concepts of security analysis.
2. Ability to design and analyze the security of security protocols.
3. Ability to take up doctoral level research work in security.

Course Contents:

Introduction: Security protocols, Security properties, Public-key certificates and infrastructures, Cryptographic hash functions, Digital signatures, Security protocol vulnerabilities, The CSP approach, Limits of formal analysis, Provable security.

Security Protocols: Needham- Schroeder public-key protocol and its security analysis, Protocols for anonymity, Anonymity and MIX networks, Fairness and contract signing, Fair exchange and contract signing protocols, Game-based verification of contract signing protocols. Yahalom protocol: Secrecy, Authentication, Non-repudiation, Anonymity; Dolev-Yao threat model.

Protocol analysis tools: Finite-state checking (Murphi), Infinite-state symbolic analysis (SRI constraint solver), Probabilistic model checking (PRISM), Game -based verification (MOCHA), Process algebras (spi-calculus and applied pi- calculus), Protocol logics (BAN, DDMP, Isabelle), Probabilistic polynomial-time calculus, CSP, B-method approach, Strand spaces, Inductive approach.

CSP: Basic building blocks, Parallel operators, Process behaviour, Modelling security protocols in CSP - Trustworthy processes, modelling an intruder, protocol goals.

Transformations: Transformations on protocols, Safe simplifying transformations, Structural transformations.

Formal analysis: Formal definitions of security for symmetric ciphers, Formal model for secure key exchange. Theorem proving - Rank functions, Secrecy of shared key, Authentication.

Text/References:

1. Peter Ryan, Steve Schneider, Michael Goldsmith, Gavin Lowe, Bill Roscoe: Modelling& Analysis of Security Protocols, Addison Wesley.
2. Stephen W. Mancini: Automating Security Protocol Analysis, Storming Media.

4. Cyber Crime, Forensics and Information Warfare(CSE634)

Course Outline: This course has a major focus on computer driven crimes, their detection, investigation, criminal laws related to the computer based crimes, and principles related to digital forensics.

Prerequisites: A course on cyber security

Course Objectives:

1. Participants of this course should be able to understand the principles of criminal laws related to computer related crimes, elements of cyber-terrorism and process of computer forensics.
2. Students should also be able to understand various aspects of cyber-crime such as motivation, investigation, cyber-attacks and defense mechanisms.
3. In addition, students, with the use of cybercrime case studies, should be able to understand various stages of forensics investigation with a focus on evidence identification and collection.

Course Outcomes:

1. Students, at the end of this course, should be able to understand the cyber-crimes, their nature, possible places of forensic artifacts, their secure collection, reporting and presentation in the court of law, and detection of fabrication and distortion of information.
2. In addition, students should be able to understand various computer forensics practices involved at various practical stages of forensic investigation.
3. Additionally, students should also understand the concepts related to attacks, their countermeasures, ethical issues and policies.

Course Contents:

Cyber Crime: Industrial espionage and cyber-terrorism, principles of criminal law, computer forensic investigation, elements of personnel security and investigations, principles of risk and security management, conspiracy in computer crime, and computer fraud investigation.
Introduction to Cyber Forensics: Computer Forensics and the law, Private &Public-sector workplace practices, Cyber Crime examples: Defacements, DoS, Credit Card theft, Silent intrusion, internal attacks, investigative actions, Forensics analysis investigative action, Computer Forensic tools.
Information Warfare: Nature of information warfare, including computer crime and information terrorism; Threats to information resources, including military and economic espionage, communications eavesdropping, computer break-ins, denial-of-service, destruction and modification of data, distortion and fabrication of information, forgery, control and disruption of information flow, electronic bombs, and psyops and perception management.
Defenses: Countermeasures including authentication, encryption, auditing, monitoring, intrusiondetection, and firewalls, and the limitations of those countermeasures. Cyberspace law and law enforcement, information warfare and the military, and intelligence in the information age. Information warfare policy and ethical issues.

Text/References:

1. Dorothy E. Denning: Information Warfare and Security, Addison Wesley.
2. Daniel Ventre: Information Warfare, Wiley.
3. Winn Schwartau: Information Warfare: Second Edition, Thunder's Mouth Press, And NY.
4. Edward Waltz: Information Warfare Principles and Operations, Artech House.

5. Public Key Infrastructure and Trust Management(CSE635)

Course objectives:

The course is designed to train the graduates in:

1. In depth understanding of Public Key Cryptography.
2. In depth understanding of Public key Infrastructure.

3. In depth understanding of security credentials.
4. To design new or modify existing cryptographic techniques.

Course Outcomes:

Graduates after completing the course shall gain:

1. In depth understanding of Public key cryptography and Infrastructure.
2. Ability to design and analyze Public Key cryptographic techniques.
3. Ability to solve network security issues in real time applications.
4. Ability to take up doctoral level research work in security.

Course Contents:

Public key infrastructure: components and architecture. PKI interoperability, deployment and assessment PKI data structures– certificates, validation, revocation, authentication, cross-certification. Repository, Certification Authority (CA) and Registration Authority (RA), trusted third party, digital certificates.

PKI services: authentication, non-repudiation, privilege management, privacy, secures communication.

Key management: certificate revocation list, root CA, attacks on CA, key backup. PKI standards – SSL, LDAP, IPsec, X.500, X.509, S/MIME

Trust models: strict v/s loose hierarchy, four corners, distributed. Certificate path processing – path construction and path validation.

Text/References:

1. AshutoshSaxena, Public Key Infrastructure, Tata McGraw Hill.
2. Carlisle Adams, Steve Lloyd. Understanding PKI: Concepts, Standards, and DeploymentConsiderations, Addison Wesley.
3. John R. Vacca. Public Key Infrastructure: Building Trusted Applications and Web Services, AUERBACH.
4. MessaoudBenantar, Introduction to the Public Key Infrastructure for the Internet, Pearson Education.

6. Digital Watermarking and Steganalysis(CSE636)

Course Objectives:

1. To be able to get Basic principles of data hiding, and the difference between steganography and watermarking.
2. To able to learn the mathematical limits of watermarking and steganography and different analysis techniques for such limits.
3. To learn about applications of different watermarking and steganography techniques used with different media objects (Stereo-objects), such as image, video, audio etc.
4. To understand Protection of Intellectual Rights to minimize the forgery, Frauds (which are the major source of funding of various criminal activities).

Course Outcome:

By the end of the course, students should be able to understand

1. How Digital watermarking and steganography works and how it can be used in applications for making it more secure?
2. Analyze and design data hiding algorithms like data embedding into multimedia.
3. Design and assess watermarking algorithms to be more robust against different attacks on digital media.
4. Different commercial and e-commerce protocols of Digital watermarking.

Course Contents:

Introduction: Information Hiding, Steganography, and Watermarking, Importance of Digital Watermarking, Steganography, Applications of Watermarking, Applications of Steganography, Properties of Watermarking Systems, Evaluating Watermarking Systems, Properties of Steganographic and Steganalysis Systems.

Models of Watermarking: Communication-Based Models of Watermarking, Geometric Models of Watermarking, Modeling Watermark Detection by Correlation, Basic Message Coding, Mapping Messages into Message Vectors, Error Correction Coding.

Watermarking with Side Information and watermark security: Informed Embedding, Watermarking Using Side Information, Dirty-Paper Codes, Robust Watermarking Approaches, and Robustness to Volumetric Distortions, Robustness to Temporal and Geometric Distortions, Security Requirements, Some Significant Known Attacks.

Steganography: Notation and Terminology, Least Bit, DCT, Spread spectrum, Information-Theoretic Foundations of Steganography, Practical Steganographic Methods, Minimizing the Embedding Impact.

Steganalysis: Steganalysis Scenarios, Some Significant Steganalysis Algorithms.

Text/References:

1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, Morgan Kauffman, Digital Watermarking and Steganography.
2. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Morgan Kauffman, Digital Watermarking principles.
3. Stefan Katzenbeisser, Fabien, and A.P. Petitcolas. Information Hiding Techniques for Steganography and Digital Watermarking, Artech House.
4. Neil F. Johnson; ZoranDuric; SushilJajodia. Information Hiding: Steganography and Watermarking - Attacks and Countermeasures, Springer.
5. Gregory Kipper. Investigator's Guide to Steganography, Auerbach Publications.

7. Data Mining and Machine Learning(CSE637)

Course Objective:

1. Demonstrate advanced knowledge of data mining and machine learning concepts and techniques.
2. To emphasize on machine learning algorithms and applications, with some broad explanation of the underlying principles.
3. To understand modern notions in data analysis oriented computing using data mining and machine learning.
4. To categorize and differentiate inputs for applying different data-mining and Machine learning techniques: frequent pattern mining, association, correlation, classification, prediction, and cluster etc.

Course Outlines:

After completing the course, student are expected to,

1. Design and implement of a data mining process for an application, including data preparation, modelling and evaluation.
2. Understand complexity of Machine Learning algorithms and their applications,
3. To access raw input data, and process it to provide suitable input for a range of data mining algorithm,
4. To be capable of performing experiments in Data mining and Machine Learning uses real-world data.

Course Contents:

Data Mining and Data Processing: Introduction and need, Descriptive and Predicative Data Mining, Data Base Schema Facts, Dimensions and Attributes, Data Base and Metadata, Data Processing-Data Cleaning, Data Integration and Transformation, Data Reduction.
Data Mining Primitives and Algorithm: Language DMQL and its Preliminary Clauses, Data Mining Methods, Association–Single and Multilevel, Characterization and Comparison, Regression Analysis, Classification and Predication, Clustering, Association, Regression, Decision Trees.
Machine Learning: Learning models: Instance based, Analytical learning, Inductive, Reinforcement and combined. Techniques: Decision tree, Artificial Neural Networks, Support Vector Machines, Bayesian learning, Bayesian belief networks, EM algorithms, k-NN, genetic algorithms, Clustering techniques.

Text/References:

1. Jiawai Han and MichelineKamber: Data Mining – Concepts and Techniques, Morgan and Kaufmann.
2. Thomas Mitchell – Machine Learning, McGraw Hill.
3. Ian H. Witten and Eibe Frank: Data Mining: Practical Machine Learning Tools and Techniques, Elsevier.
4. Bramer: Principles of Data Mining, Springer.
5. Pang-Ning Tan, M. Steinbach, V. Kumar: Introduction to Data Mining, Addison Wesley.
6. Ryszad S. Michalski, Ivan Bratko, MiroslavKubat (Editors): Machine Learning and Data Mining: Methods and Applications, Wiley.

8. Simulation and Modeling (CSE638)

Course Objectives:

1. To understand students to basic simulation methods and tools for modelling and simulation.
2. To get knowledge and skills in the area of simulation and modeling, and highlight their applications in different areas.
3. To understand modeling concepts, design, simulation, verification and validation.
4. To be able to demonstrate the usefulness of simulation as a tool for problem solving methods.

Course Outcomes:

After learning this course, the students are expected to

1. To be able to solve real world problems by using various modeling techniques this cannot be solved strictly by mathematical approaches.
2. Be able to describe the components of continuous and discrete systems and simulate them.
3. Get knowledge of simulation principles and hence ability to create simulation models of various types.

Course Contents:

Definition of a system, System concepts, type of system, continuous & discrete systems, modeling process verification & validation.
Markov chains. Weak law of large numbers. Central limit theorem. Strong law of large numbers. Queuing models: Little's Theorem, M/M/1, M/M/m, M/M/', M/M/m/m, M/G/1, and M/M/1/J queuing systems.
Introduction, classification of simulation models, advantages and disadvantages of simulation.

Discrete system simulation: Monte Carlo method, Random number generators. Probability Distributions.
Element of inventory theory, more complex inventory models, finite and infinite delivery rate model with and without back ordering, Simulation of inventory systems.

Text/References:

1. System simulation, Gorden G., Prentice Hall of India
2. System simulation, NarsingDeo, McGraw Hill.
3. Simulation modeling and analysis, Law and Kelton, McGraw Hill.

9. Optimization Techniques(CSE639)

Course Objectives:

1. General understanding of optimization under constraints.
2. Develop knowledge and skills in linear and integer programming (LP&IP) and their applications.
3. Knowledge and implementation of discrete optimization problems and their algorithms
4. Application of optimization tools in different domains of computing and data science

Course Outcomes:

1. Be able to formulate Transportation/Assignment problems as LP problems and solve those using LP solvers.
2. Be able to mathematically formulate some "real" problems as continuous and discrete optimization problems.
3. Be able to distinguish between continuous and discrete cases. Further, should be able to understand integer and 0/1 programming formulations.

Course Contents:

Introduction: Introduction, Engineering applications (models) of optimization.
Linear Programming: Linear programming problem, graphical, simplex method, Concept of duality, Dual simplex method.
Transportation Problems: basic feasibility solution by different methods, optimal solution, Degeneracy in transportation problem, unbalanced transportation problems.
Assignment Problems: Balanced and unbalanced assignment, assignments to given schedule. Introduction to Non-linear programming.

Text/References:

1. Rao S S, Optimization: Theory and Applications.
2. N.S. Kambo : Mathematical Programming Techniques, East West Press
3. Hamdy A. Taha : Operation Research an Introduction, PHI
4. VasekChvatal: Linear Programming, W.H. Freeman & Co.
5. Walsh G R, Methods of Optimization
6. Papadimitriou, Stieglitz: Combinatorial Optimization: Algorithms and Complexity, PHI.

10. Topics in Operating Systems (CSE640)

Course Outline:
Topics in OS course aims to deliver various advanced topics related to distribute operating systems, related aspects, algorithms and research issues.

Prerequisites:
Courses on Operating Systems and Computer Networks

Course objectives:
1. To understand the ingredients of a distributed systems and its relation with computer networks and stand-alone operating systems.
2. To learn and implement the concepts such as distributed shared memory and distributed file systems.
3. To understand the concepts such as distributed transaction and concurrency, distributed file systems, scheduling, election, and performance and security issues.

Course Outcomes:
1. At the end of this course, students should be able to understand the fundamentals of distributed operating systems and advanced topics such as resource allocation, fault tolerance and caching issues.
2. With the help of a strong practical lab component student should be able to understand the implementation and programming of any one or two distributed systems/ file systems.

Course Contents:
UNIT 1: Introduction to Operating Systems, Processes and Threads, System calls, IPC mechanisms (pipe,
fifo, signals), Memory and file management.
UNIT 2: Introduction to Distributed systems, Hardware and Software Concepts, Communication, Layered Protocols, Remote Procedure Call, Remote Object Invocation, Distributed File Systems, Cryptographic File Systems, Log Structured File Systems, Distributed Shared Memory.
UNIT 3: Distributed System Concepts: Code Migration and Software Agents. Naming, Locating Mobile
Entities, Removing Unreferenced Entities, Synchronization, Clock Synchronization, Logical Clocks,
Global State and Election Algorithms, Consistency, Replication, Fault Tolerance, Resource Allocation, Process Resilience, Reliable Client-Server Communication, Distributed Concurrency and Transactions, Group Communication, Distributed Commit and recovery.
UNIT 4: Operating System Security: Access Control, Hardening, Logging, Virtualization, sandboxing, protection of execution space and research topics.

Text/References:
1. Tanenbaum: Distributed Operating Systems, Pearson Education.
2. Bach, Design of Unix O/S.
3. Coulouris et al, Distributed Systems: Concepts and Design, Addison Wesley.
4. Tanenbaum and Steen: Distributed Systems: Principles and Paradigms, Pearson Education.
5. Some research and survey papers.

11. Topics in Computer Architecture (CSE641)

Course objectives:
The course is designed to train the graduates in:

1. Advanced topics in architecture of digital computers.
2. Usage of digital computers in industry and research.
3. High performance computing.

Course Outcomes:
Graduates after completing the course shall gain:

1. Ability to understand architecture of digital computers.
2. Ability to apply digital computers in solving complex problems in industry and research.
3. Ability to apply high performance computing in real world applications.

Course Contents:
Introduction to Computer Architecture: Von Newman architecture, basic components, memory hierarchy, instruction cycle, I/O processing; ALU, microinstructions and Control unit, RISC design versus CISC design.
Instruction level parallel processors: Pipelining (instruction and arithmetic), hazards in pipelining, Pipeline scheduling (static and dynamic), Throughput improvement, VLIW architectures. Instruction level data-parallel architectures: SIMD, vector architectures.
Multiprocessor architectures: Interconnection networks, shared and distributed memory, cache coherence, scheduling and load balancing, scalable multiprocessor.
Data Flow computers: Introduction, Data Flow Program Graph, Activity Template, Scheme, Implementation, and Pipelining in Data Flow.

Text/References:

1. Hennessy and Patterson. Computer Architecture – A Quantitative Approach. Morgan Kauffman.
2. Culler, Singh and A. Gupta. Parallel Computer Architecture, Sima and Fountain, Morgan Kauffman.
3. Hwang and Briggs. Computer Architecture and Parallel Processing, McGraw Hill.
4. Hwang, Advanced Computer Architectures, Tata McGraw Hill.

12. Advanced Compiler Design (CSE642)

Course Description:
Topics including foundations of data-flow analysis, use of dataflow analysis for program optimization, code generation across basic blocks, interprocedural and intra procedural analysis and adaptive compilers are described.

Course Objective:

- To focuses on the interpretation and compilation techniques needed to obtain high performance on modern computer architectures.
- To provides experience with implementation issues by using programming project and,
- To allows students to evaluate the impact of many of the techniques covered in the course in the context of an actual ``real-world'' compiler.

Course Outcomes:
Graduates after completing the course shall gain:

- Ability to explore the basic techniques and a variety of program analysis and code refactoring tools.

- Ability to understand optimizing compilers, program verifiers, bug fingers, garbage collectors, and runtime monitoring systems.
- Students are able to find out research in the area of program analysis and compilers through case studies and getting small project.

Course Outlines:

A Tour of Compiler Design**,** Phases of Compilation – Lexical Analysis, regular grammar and regular expression, LEX lexical analyzer generator, Top down Parsing, Bottom up parsing, YACC – automatic parser generator.
Syntax directed definition, L- Attributes, Bottom up evolution of inherited attributes, Construction of Syntax tree, Top down translation, Intermediate languages, Assignment statements, and Code generator design issues.
Abstract Syntax Tree, Basic Blocks, Control Flow Graph, Dataflow Graph, Static Single Assignment, Control Dependence Graph, Program Dependence Graph, Dataflow Analysis, Optimization of Basic Blocks, Loop optimizations, Global Register Allocation, and Instruction Scheduling.
Case studies of compilers and future trends and selected papers from the literature.

Text/References:

1. Aho, R. Sethi, Ullman: Compilers: Principles, Techniques and Tools, Addison-Wesley.
2. Modern Compiler Implementation in C- Andrew N. Appel, Cambridge University Press.
3. Steven Muchnick: Advanced Compiler Design & Implementation, Morgan Kaufmann.
4. Lex&yacc – John R. Levine, Tony Mason, Doug Brown, O'reilly.
5. Modern Compiler Design- Dick Grune, Henry E. BAL, Cariel T. H. Jacobs.

13. Advanced Topics in Databases(CSE643)

Course Objective:

1. To understand the underlying computer system on the database system.
2. To get an understanding of the internals of the storage and retrieval components of the database.
3. To focuses on how information is transformed into various implementation techniques used in real system.

Course Outcomes:

Graduates after completing the course shall gain:

1. Ability to analyze an information storage problem and derive an information model.
2. Use database package to create, populate, maintain, and query database.
3. Understanding of programmatic interfaces to a database and be able to use the basic functions of one such interface.

Course Contents:

Query Processing and Query Optimization: Storage and File structure and Indexing, Measures of query cost, Cost estimation of selection operation, sorting, join etc., Query Optimization in Relational expressions, Estimating statistics of expression result, Choice of evaluation plans, Materialized views.
Transaction Management: Transactions, Concurrent executions, Testing serializability, Concurrency control, Timestamp based and Lock based protocols, Deadlock handling, Recovery and Atomicity, Log-based Recovery.
Distributed Databases: Principles, Architecture, Design, Distributed query processing, Transaction Processing, Concurrency control, Integrity and Security.
Database System Architecture: Client/server architecture, Parallel Databases, Web databases, Temporal Databases, Multimedia Databases, and case studies.

Text/References:

1. Silberschatz A, Korth HF, Sudarshan S, Database System Concepts, McGrall Hill.
2. Elmasri R and Navathe SB, Fundamentals of Database Systems, 3rd Edition, Addison Wesley,2000.
3. Ceri S, Pelagatti G, Distributed Databases – Principles and Systems, McGraw Hill.
4. Khashafian S and Baker AB, Multimedia and Imaging Databases, Morgan Kaufmann.
5. M.Tamer, Özsu, Principles of Distributed Database Systems, Second Edition,
6. Raghu Ramakrishnan, Database Management Systems, McGraw-Hill, 2000

14. Mobile Computing(CSE644)

Course objectives:
The course is designed to train the graduates in:

1. In depth understanding of Wireless and Mobile Communications.
2. In depth understanding of techniques and protocols in Mobile Communications.
3. To design new or modify existing techniques in Mobile Communications.

Course Outcomes:
Graduates after completing the course shall gain:

1. In depth understanding of Wireless and Mobile Communications.
2. Ability to design and analyze Mobile Communication techniques.
3. Ability to solve communication issues in real time applications.
4. Ability to take up doctoral level research work in Wireless and Mobile Communications.

Course Contents:
Introduction to mobile computing: principles, classification & overview of devices, operating systems. Wireless transmission: brief overview, multipath propagation, hidden & exposed terminals. Medium access control & protocols: SDMA, FDMA, TDMA, DAMA, FAMA, PRMA, Reservation TDMA, polling, CSMA/CA, CDMA etc.
Wireless LAN: infrastructure & ad-hoc networks, IEEE 802.11, HIPERLAN. Mobile network layer: mobile IP, DHCP, infrastructure & Ad-hoc routing.
Mobile transport layer: indirect TCP, snooping TCP, mobile TCP etc. mobile support, WWW & mobility, WAP.

Text/References:

1. Principles of mobile computing Hansmann&Merk., Springer
2. Mobile communications Jochen Schiller , Pearson
3. 802.11 wireless networks Matthew S.Gast, O'REILLY.
4. Wireless LANs: Davis & McGuffin, McGraw Hill
5. Mobile Communications Handbook by Jerry D. Gybson
6. Mobile Communications Handbook by Raymond Steel

15. Advance Software Engineering(CSE645)

Course Description: This course discusses the advances in Software Engineering. It includes the technical aspects and the issues pertaining to Software Project Management. It will enable the learners to apply Software testing techniques in real life scenarios.

Course Objectives
The course aims to:
1. Introduce the concepts of DFDs and Decision trees.
2. Demonstrate the use of Unified Modeling Language.
3. Develop understanding of Gantt chart, PERT and CPM.
4. Cover how software testing can be done.

Course Outcomes
At the end of the course, the student will be able to:
1. Select appropriate software development process.
2. Do project scheduling and project management.
3. Perform software testing using different testing techniques and generate test cases.

Course Contents:

Software Engineering Concepts and Methodologies: Agile Software Development, Extreme Programming, Scrum, RUP; Data Flow Diagrams, Decision Table, Decision Tree; Design Patterns and Unified Modeling Language. Case studies
Software Project Management: Project Scheduling, Work breakdown structure, Gantt chart, PERT, CPM; Software Metrics for Object-Oriented systems; Software Quality & Reliability Standards, Capability Maturity Models-CMM and CMMI, Six Sigma Concept for Software Quality.
Software Testing: Software Testing Techniques and Strategies; Flow graphs and Path Testing; Test case Generation; Security Testing; Testing tools.
Formal Methods and Cleanroom Engineering: Basic concepts, mathematical preliminaries, applying mathematical notations for formal specification, languages, using Z to represent an example software component.
Text/References:

1. Sommerville, Ian, Software Engineering, Addison-Wesley Publishing Company, (2006) 8th ed.
2. Boris Beizer, Software Testing Techniques, John Wiley &Dreamtech (2002).
3. Software Metrics: A rigorous and Practical Approach by Norman E. Fenton and Shari Lawrence Pfleeger, International Thomson Computer Press (1997) 2nd ed.
4. Pressman, Roger, Software Engineering - A Practitioners Approach, McGraw Hill (2008) 6th ed.

16. Multimedia System and Security(CSE646)

This course will enable learners in developing basic understanding of multimedia and its security aspects. It will cover an introduction to multimedia, its applications and quality of service. It will also discuss the security and forensic issues related to multimedia.

Course Objectives
The course aims to:
1. Introduce multimedia, its application areas, data encoding and compression techniques.
2. Develop understanding of Quality of Service and its constraints.
3. Understand synchronization concepts.
4. Discuss multimedia security attacks and defense techniques.

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

1. Demonstrate how quality of service can be ensured in multimedia applications.
2. Apply different synchronization techniques on multimedia.
3. Ensure security of multimedia applications.

Course Contents:

Introduction: Multimedia Application Areas, Interdisciplinary Aspects of Multimedia, like animation, motion and shape tween, Multimedia Data Encoding, Concept of data compression in multimedia field (lossless and lossy compression techniques).

Quality of Service & Operating System: Requirements and Constraints, Quality of Services Concept, Resource Management, Establishment Phase (QoS Translation, QoS Scaling, QoS Routing,), Media Server Architecture, Storage Management, Services, Protocols, Layers.

Synchronization: Synchronization, Intra- and Inter-object Synchronization, Time-dependent Presentation Units, Special Methods for Multimedia Synchronization, Case Studies.

Security in Multimedia Applications: Security attacks, Multimedia Encryption, Steganography, Digital image watermarking, Watermarking vs. Digital Signature, Multimedia Authentications, Multimedia Forensic, and Introduction to Video Coding.

Text/References:

1. Ralf Steinmetz, KlaraNahrstedt. *Multimedia Systems*, Springer International Edition
2. John. F. Koegel Buford. *Multimedia Systems*. Pearson Education.
3. Digital Watermarking and Steganography **By**Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich and TonKalker, Elsevier, ISBN: 978-0-12-372585-1
4. Communications and Multimedia Security Issues by Ralf Steinmetz, Springer
5. Khalid Shayood, Data Compression.

17. Secure Programming Techniques(CSE647)

Course Outline: This course focuses on programming techniques to write secure and safe code toenable secure systems. The course should be aided with a strong lab component utilizing the concepts delivered in the lectures.

Prerequisites: Course on programming and security.

Course Objectives:

1. Student in this course should learn the need of security while coding and methods of implementing secure design principles.
2. Student should understand the need of risk analysis, threat modeling and their mapping in the resultant code with proper documentation.
3. Student should understand the importance to adhere to the safe-code guidelines and learn defensive coding techniques with safe and secure use of crypto APIs.

Course Outcomes:

1. At the end of this course, students should be able to understand the need of secure software design and problems of insecure codes.
2. In addition, as a major focus, students should understand the need of secure code, CVE and CWE guidelines, common mistakes, defensive coding principles, proper and improper use of random number generators, key generation and storage, selection of proper algorithm and related specifications and handling permissions.

Course Contents:

Introduction: Security, CIA Triad, Viruses, Trojans, and Worms In a Nutshell, Security Concepts- exploit, threat, vulnerability, risk, attack. Malware Terminology: Rootkits, Trapdoors, Botnets, Key loggers, Honeypots, Active and Passive Security Attacks, SQL injection, ARP Spoofing and its countermeasures.
Need for secure systems: Proactive Security development process, Secure Software Development Cycle (S-SDLC), Security issues while writing SRS, Development Phase, Test Phase, Maintenance Phase, Writing Secure Code – Best Practices SD3 (Secure by design, default and deployment).
Threat modelling process and its benefits: Identifying the Threats by Using Attack Trees and rating threats using DREAD, Risk Mitigation Techniques and Security Best Practices, Security techniques.
Security Issues in C Language: String Handling, Code Injection Attacks, Canary based countermeasures using Stack Guard, Optimization Techniques, Aspect and Aspect Oriented Programming, Insecure Coding Practices in Java Technology, Dangling Reference, Garbage Collection, and Java Case Study.

Text/References:

1. Writing Secure Code, Michael Howard and David LeBlanc, Microsoft Press, 2nd Edition, 2004
2. Buffer Overflow Attacks: Detect, Exploit, Prevent by Jason Deckard ,Syngress,1st Edition, 2005
3. Threat Modeling, Frank Swiderski and Window Snyder, Microsoft Professional, 1st Edition ,2004

18. Network Protocols(CSE648)

Course Outline: This course focuses on detailed understanding of various network protocols with a focus on their performance, parameters, security, and state of the art implementations.

Prerequisites: Computer Networks

Course Objectives:

1. Students in this course should learn important network protocols with their specifications from the agencies in the form of white papers, RFCs and possible configuration issues changing their performance.
2. In addition, students should also understand the possible usages of such protocols, performance, scalability and overhead issues, their security analysis, possible attacks and defense mechanisms.
3. Students should also take an aid from lab component to use the real implementation of such protocols and apply possible concepts applicable.

Course Outcomes:

1. At the end of this course, students should be able to understand the need and methods of protocol design, analysis and modeling for suitable performance calibrations.
2. In addition, students should also understand the needs of protocol standards, RFCs and need of protocol evaluation, simulation, and security analysis tools.

Course Contents:

1. Application Layer Protocols - Introduction to Application Layer Protocols, BooTP, S-HTTP, IMAP & IMAP2, NAT, NTP,Rlogin, SLP.

2. Transport Layer Protocols - ITOT, RDP, RVDP, TALT, RPC, RTPS, VRRP
3. Network Layer Protocols - BGP, EGP, IPv6, NARP, OSPF, RIP, BGMP, IGMP, MARS, IPX, Bitcoin
4. Data link Layer Protocols - ARP, InARP, IPCP, Ipv6ED, IGMP, MARS
5. LAN, MAN, WAN, ATM, SONET, WLAN, SNAP, STP, FC, FCP, FLIP, Local Address Resolution, Remote Delivery, Remote Address Resolution
6. IEEE 802.11 aka Wireless LAN (Wi-Fi Certification), System Network Architecture

Text/References:

1. Network Protocols Handbook – Jawin Technologies, Inc.
2. 802.11 Wireless Network Matthew S. Gast, O'REILLY.
3. The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference
4. Ethernet: The Definitive Guide – Charles E Spurgeon
5. Related online resources

19. Cloud Computing (CSE649)

Course Outline:
The course on Cloud Computing will enable the students to understand the aspects of this emerging and growing computing paradigm with various ingredients such as cloud computing service models, virtualization technology, and practical aspects such as security and implementation issues.

Course Objectives:

1. To learn the fundamentals of cloud computing, its architecture, and various service levels.
2. To understand the formal model of virtualization and various virtualization techniques.
3. To equip students with cloud application frameworks, auto-scaling and resource allocation strategies and related open issues.
4. To understand the state of the art cloud security issues and solutions in cloud computing.

Course Outcomes:

1. At the end of this course, students should be able to understand, design and configure various cloud services at the level of infrastructure, software, and platform.
2. With the help of a strong lab component, students should be able to setup cloud infrastructures using software such as OpenStack or Eucalyptus.
3. Understanding of cloud security and dependencies on CSP and possible solutions.
4. Cloud adoption decision making for different case studies and understanding of SLAs.

Course Contents:

Introduction: Introduction to various computing paradigms, cluster computing, grid computing, autonomic computing, introduction to cloud Computing, various layers of cloud computing services (Software, Infrastructure, and Platform), cloud architecture, challenges and risks.

Virtualization: Formal model of virtualization, virtual machine monitors (Xen, VirtualBox, VMware etc.), virtual appliances, VM provisioning, Cloning and Snapshots, VM Backup and Recovery, VM migration, and Inter-operability Issues.

Cloud Computing Services: IaaS, PaaS and SaaS services and case studies (OpenStack, GFS, MapReduce, BigTable etc.). Application Migration to Cloud, Auto-scaling and on-demand resource allocation schemes, Cloud Service Level Agreement (SLA), SLA monitoring, accounting and verification, data center automation and containers.

Cloud Security: Cloud Security Challenges and Risks, Data Security, Application Security, Virtual Machine Security, Cross-VM attacks, Identity Management and Access Control, Establishing Trusted Cloud computing, Cloud Storage security, deduplication and Disaster Recovery in Clouds.

Text/References:

1. Hwang, Kai, Jack Dongarra, and Geoffrey C. Fox. Distributed and cloud computing: from parallel processing to the internet of things. Morgan Kaufmann, 2013.
2. Cloud Computing Bible, Barrie Sosinsky, Wiley-India, 2010
3. Buyya, Rajkumar, James Broberg, and Andrzej M. Goscinski, eds. Cloud computing: Principles and paradigms. Vol. 87.John Wiley & Sons, 2010.
4. Krutz, Ronald L., and Russell Dean Vines. Cloud security: A comprehensive guide to secure cloud computing. Wiley Publishing, 2010.
5. Various survey and research papers.

20. Parallel Processing (CSE650)

Course Objectives:

1. To understand various kinds of mathematical models of parallel computational system.
2. Students will be able to understand architectural design that provides the parallel computational power to the computer.
3. To equip students with parallel processing application frameworks, architecture, resource allocation strategies and related open issues.

Course Outcomes:

1. Ability to understand uniprocessor computer architecture, understanding the computer architecture (i.e., pipelining and superscalar processor design and memory hierarchy).
2. To be able to design parallel architecture hardware and parallel software.
3. Understand the concepts of shares-memory management, distributed-memory with MPI and general-purpose GPU

Course Contents:

Pipeline and Vector Processing: Nonlinear and linear pipelining, Multiprocessor, Multicomputer, Super computer, Array Processors, Scope and Application of Parallel approach.
Paradigms of parallel computing: SIMD, Systolic; Asynchronous - MIMD, reduction paradigm, Hardware taxonomy, Flynn classifications, Handlers classifications.
PRAM model and its variants: EREW, ERCW, CRCW, PRAM algorithms, Sorting network, Interconnection RAMs, Parallelism approaches - data parallelism, control parallelism.
Parallel Processors: Taxonomy and topology - shared memory multiprocessors, distributed memory networks, Processor organization - Static and dynamic interconnections. Embedding and simulations.
Performance Metrics: Laws governing performance measurements. Metrics - speedup, efficiency, utilization, cost, communication overheads, single/multiple program performances, bench marks.

Text/References:

1. M. J. Quinn. Parallel Computing: Theory and Practice, McGraw Hill, New York, 1994.
2. T. G. Lewis and H. El-Rewini. Introduction to Parallel Computing, Prentice Hall, New Jersey, 1992.
3. T. G. Lewis. Parallel Programming: A Machine-Independent Approach, IEEEComputer Society Press, Los Alamitos.
4. Sima and Fountain, Advanced Computer Architectures, Pearson Education.
5. Mehdi R. Zargham, Computer Architectures single and parallel systems, PHI.

6. Ghosh, Moona and Gupta, Foundations of parallel processing, Narosa publishing.
7. Ed. Afonso Ferreira and Jose' D. P. Rolin, Parallel Algorithms for irregular problems -State of the art, Kluwer Academic Publishers.
8. Selim G. Akl, the Design and Analysis of Parallel Algorithms, PH International.

21. Digital Image Processing (CSE651)

Course Outlines:
The course focuses on basic and essential topics in Digital Image Processing, including Pixels, Pre Processing of images, Image Restoration, Segmentation, Morphological Properties and Pattern Recognition.

Course Objectives:
1. To understand various kinds of mathematical models to perform imaging operations.
2. Demonstrate the various kinds of operations on different images for various applications.
3. Work on real time applications like segmentation, restoration, object detections, bio-metric application.

Course Outcomes:
Graduates after completing the course shall gain:

1. Ability to enhance student skill in digital image processing, emphasizing problem solving techniques such as collecting data, find out features, recognizing patterns, and numeric computations exercises.
2. Ability to establish a strong and meaningful bridge with images, signals and computer science.
3. To enable students to develop their problem-solving skills, hands-on experience with concepts and enhance the opportunity for taking up research challenge.

Course Contents:
The Digitized Image and its Properties: Applications of image processing, image function, image representation, sampling, quantization, color images, metrics and topological properties of digital images, histograms, image quality, noise image.
Image Pre-processing: Pixel brightness transformation, geometric transformation, local pre-processing-image smoothening, scale in image processing, spatial operation, intensity transformation and spatial filtering, color models, gray scale transformation.
Image Restoration & Segmentation: Image degradation and re-storage process, segmentation, Point, line and edge detection, threshold detection methods, parametric edge models, edges in multi spectral images, Region based segmentation, image representation, border following and chain codes, boundary descriptors, regional descriptors.
Pattern Recognition Fundamentals: Basic concepts of pattern recognition, fundamental problems in pattern recognition system, design concepts and methodologies, example of automatic pattern recognition systems, a simple automatic pattern recognition model.

Text/References:
1. Digital Image Processing: Rafel C. Gonzalez Richard E. Woods, Second edition, Addison-Wisley.
2. Digital Image Processing: A K Jain, PHI
3. R. M. Haralick, L. G. Shapiro. Computer and Robot Vision. Addison-Wesley, 1993.
4. A. Rosenfeld, A. C. Kak. Digital Picture Processing. Addison-Wesley, 1983
5. D. A. Forsyth, J. Ponce. Computer Vision: A Modern Approach. Prentice-Hall, 2003.
6. Pattern Recognition and Image Analysis: Earl Gose, Richard Johnson Baugh, Prentice Hall of India Private Limited, 1999.
7. Pattern Recognition principles: Julus T. Tou and Rafel C. Gonzalez, Addison –Wesley publishing company.

22. Biometrics and Security (CSE652)

Course Outlines: Biometrics is about how we can recognize people automatically, by personal characteristic like fingerprints and faces etc. Information needs to sense it and then deliver an assessment of the identity associated with that data. This course covers the uses and applications of biometrics and how to undertake basic research in biometrics using case studies including biometric recognition system like Face, Signature, Fingerprint, Iris, Tongue recognition etc.
Course Objective:
The course aims to:
Assess ways of how we identify people, identify different environments for biometric use, define biometrics.
To understand various kinds of biometric systems, securities and Recognition systems.
The newest approaches to biometrics and how they fit in its technological landscape

Course Outcomes:
At the end of the course, the student will be able to:
Future emerging trends in the biometrics industry.
Identify algorithms for finger, face, iris and tongue biometric technology.
Ability to take up research work in Biometric like face recognition, tongue recognition systems.
Corse Contents:
Introduction of Biometrics: history, applications, performance evaluation, Biometric system design challenges, basic image operations, edge detection in digital images, filtering, sharpening etc.
Biometric system: identification and verification, FAR/FRR, system design issues, positive / negative identification, authentication protocols, matching score distribution, FAR/FRR curve, expected overall error, EER.
Biometric system security: Biometric attributes types, verification and identification on multimodal system, normalization strategy, fusion methods, Biometric system security, and vulnerabilities.
Recognition systems: general description, features, types of algorithms used for interpretation, components and operations for Face, Signature, Fingerprint, Iris, Tongue etc.
Text/References:
Guide to Biometrics, By: Ruud M.Bolle,SharathPankanti, Nalini K. Ratha,Andrew W. Senior, Jonathan H. Connell,Springer 2009
Biometrics, Woodward, J.D. and Orlans, Nicholos M., McGraw Hill (2002)

1. Digital Image Processing using MATLAB,By: Rafael C. Gonzalez, Richard Eugene Woods, 2nd Edition, Tata McGraw-Hill Education 2010
2. Biometric Solutions for Authentication in an e-World, Zhang, D., (Ed.), Kluwer Publisher, 2002.
3. BIOMETRICS: Personal Identification in Networked Society, A. Jain, R. Bolle, S. Pankanti, (Ed.), Kluwer Academic Publishers, 1999. ISBN 0-7923-8345-1. TK7882.P3 B36
4. Other Research Papers.