CURRICULUM & SYLLABI

M.Tech (Computer Science and Information Security)

COMPUTER SCIENCE & ENGINEERING

Effective from AY: 2024-25



NATIONAL INSTITUTE OF TECHNOLOGY WARANGAL

WARANGAL, TELANGANA

Table of Contents

VISION AND MISSION OF THE INSTITUTE 3
VISION AND MISSION OF THE DEPARTMENT 3
PROGRAM EDUCATIONAL OBJECTIVES 4
PROGRAM OUTCOMES 5
CURRICULUM 6
SYLLABI 10

National Institute of Technology Warangal

Vision and Mission of the Institute

VISION

Towards a Global Knowledge Hub, striving continuously in pursuit of excellence in Education, Research, Entrepreneurship and Technological services to the society

MISSION

- Imparting total quality education to develop innovative, entrepreneurial and ethical future professionals fit for globally competitive environment.
- Allowing stake holders to share our reservoir of experience in education and knowledge for mutual enrichment in the field of technical education.
- Fostering product-oriented research for establishing a self-sustaining and wealth creating centre to serve the societal needs.

Vision and Mission of the Department

Computer Science & Engineering

VISION

Attaining global recognition in Computer Science & Engineering education, research and training to meet the growing needs of the industry and society.

MISSION

- Imparting quality education through well-designed curriculum in tune with the challenging software needs of the industry.
- Providing state-of-art research facilities to generate knowledge and develop technologies in the thrust areas of computer science and engineering.
- Developing linkages with world class organizations to strengthen industry-academia relationships for mutual benefit.

Program: M.Tech, Computer Science and Information Security

Program Educational Objectives

PEO-1	Apply knowledge of computer science to provide information security.
PEO-2	Design and develop secure software systems using models as per user requirements.
PEO-3	Work in teams using common security tools and environment to achieve project objectives.
PEO-4	Communicate effectively, demonstrate leadership qualities and exhibit professional ethics.
PEO-5	Engage in lifelong learning to adapt to changing professional and societal needs for career advancement.

Program Articulation Matrix

PEO / Mission Statements	PEO-1	PEO-2	PEO-3	PEO-4	PEO-5
Imparting quality education through well- designed curriculum in tune with the challenging software needs of the industry	2	3	2	2	2
Providing state-of-art research facilities to generate knowledge and develop technologies in the thrust areas of computer science and engineering	1	1	3	2	1
Developing linkages with world class organizations to strengthen industry-academia relationships for mutual benefit.	2	3	2	1	1

1 - Slightly; 2 - Moderately; 3 - Substantially

Program: M.Tech, Computer Science and Information Security

Program Outcomes

PO1	Engage in critical thinking and pursue investigations / research and development to solve practical problems.
PO2	Communicate effectively, write and present technical reports on complex engineering activities by interacting with the engineering fraternity and with society at large.
PO3	Demonstrate higher level of professional skills to tackle multidisciplinary and complex problems related to information security.
PO4	Specify secure protocols for safe handling the digital assets and for exchange of information among entities in the real world.
PO5	Design algorithms for secure multi-party computations and analyze their complexities.
PO6	Evaluate alternative designs of secure systems focusing on efficiency, scalability and cost parameters with compliance to legal, privacy and ethical issues of the operational field.

CURRICULUM
Program: M.Tech. (Computer Science and Information Security)

1st Semester

S.No.	Code	Course Title	L-T-P	Credits
1	CS26001	Advanced Algorithms	3-0-0	3
2	CS26003	Foundations of Cryptography	3-0-0	3
3	CS26005	Data Mining	3-0-0	3
4	CS260XX	Professional Elective – I	3-0-0	3
5	CS260XX	Professional Elective – II	3-0-0	3
6	CS26007	Cryptography Laboratory	0-0-3	2
7	CS26009	Data Mining Laboratory	0-0-3	2
			Total Credits	**19**

2nd Semester

S.No.	Code	Course Title	L-T-P	Credits
1	CS26002	Network Security	3-0-0	3
2	CS26004	Data Privacy	3-0-0	3
3	CS260XX	Professional Elective - III	3-0-0	3
4	CS260XX	Professional Elective - IV	3-0-0	3
5	CS260XX	Professional Elective - V	3-0-0	3
6	CS26006	Network Security Laboratory	0-0-3	2
7	CS26008	Data Privacy Laboratory	0-0-3	2
8	CS26095	Minor Project	0-0-0	2
			Total Credits	**21**

3rd Semester

S.No.	Code	Course Title	L-T-P	Credits
1	CS26089	Seminar and Technical Writing	0-0-0	2
2	CS26091	Summer Internship/Research Experience	0-0-0	2
3	CS26093	Comprehensive Viva-Voce	0-0-0	2
4	CS26097	Dissertation: Part A	0-0-0	8
			Total Credits	**14**

4th Semester

S.No.	Code	Course Title	L-T-P	Credits
1	CS26098	Dissertation: Part B	0-0-0	12
			Total Credits	**12**

Professional Elective Courses:

Professional Elective-I/II				
S.No.	**Code**	**Course Title**	**L-T-P**	**Credits**
1	CS26021	Biometric Security	3-0-0	3
2	CS26023	Computability and Complexity	3-0-0	3
3	CS26025	Digital Video Processing	3-0-0	3
4	CS26027	Cryptanalysis	3-0-0	3
5	CS26029	Information Security and Secure Coding	3-0-0	3
6	CS26031	Information Systems Control and Auditing	3-0-0	3
7	CS26033	Mathematical models for Internet	3-0-0	3
8	CS26035	Probabilistic Algorithms	3-0-0	3
9	CS26037	Secure Cloud Computing	3-0-0	3
10	CS26039	Secure Software Engineering	3-0-0	3
11	CS26041	Unix Internals	3-0-0	3
12	CS26043	Web and Database Security	3-0-0	3

Professional Elective-III/ IV/ V				
S.No.	**Code**	**Course Title**	**L-T-P**	**Credits**
1	CS26022	Algorithmic Coding Theory	3-0-0	3
2	CS26024	Cyber crime and Information Warfare	3-0-0	3
3	CS26026	Cyber laws and Intellectual Property Rights	3-0-0	3
4	CS26028	Cyber Security	3-0-0	3
5	CS26030	Data Hiding	3-0-0	3
6	CS26032	Deep Learning	3-0-0	3
7	CS26034	Digital Forensics	3-0-0	3
8	CS26036	Foundations of Blockchain Technology	3-0-0	3
9	CS26038	Information Security Risk Management	3-0-0	3
10	CS26040	IoT Security	3-0-0	3

11	CS26042	Privacy and Security for online social networks	3-0-0	3
12	CS26044	Privacy Enhancing Technologies	3-0-0	3
13	CS26046	Public Key Infrastructure and Trust Management	3-0-0	3
14	CS26048	Scripting languages for information security	3-0-0	3
15	CS26050	Secure Dependable and Distributed Computing	3-0-0	3
16	CS26052	Secure Operating Systems	3-0-0	3
17	CS26054	Secure Protocols for Electronic Commerce	3-0-0	3
18	CS26056	Security of E-Based Systems	3-0-0	3
19	CS26058	Wireless and Mobile Networks	3-0-0	3

SYLLABI

M.Tech. (Computer Science and Information Security)

1st Semester

CS26001 **3-0-0 (3)**

Advanced Algorithms

Pre-Requisites: **None**

Course Outcomes:

CO-1	Analyze worst-case running times of algorithms using asymptotic analysis.
CO-2	Classify problems into different complexity classes corresponding to deterministic, approximation and parameterized algorithms.
CO-3	Analyze the complexity of graph problems for different graph classes.
CO-4	Analyze approximation algorithms and determine approximation factor.
CO-5	Design and analyze efficient randomized algorithms.

Course Articulation Matrix:

	PO-1	**PO-2**	**PO-3**	**PO-4**	**PO-5**	**PO-6**
CO-1	3	-	3	3	-	-
CO-2	3	-	3	3	-	-
CO-3	3	-	3	3	-	-
CO-4	3	-	3	3	-	-
CO-5	3	-	3	3	-	-

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Average case analysis of algorithms, Correctness of Master Theorem, Selection in Worst Case Linear Time, Large integer multiplications using FFT, Dynamic Programming - Matrix Chain Multiplication Problem, Optimal Binary Search Tree, Linear Algorithm for Domination in Trees, Maximum Cardinality Search and Chordal Graphs, Greedy Algorithm for Optimal Coloring of Chordal Graphs, NP-completeness, Efficient Reduction Proofs via Examples, Domination in Subclasses of Bipartite Graphs and Chordal Graphs, Exact Exponential Algorithm for Domination Problems, Treewidth, Parameterized Complexity Classes, APX hardness and APX-completeness, Approximation Algorithm for Connected Dominating Set Problem, The Stable Marriage Problem, The Coupon Collector`s Problem.

Learning Resources:

Text Books:

1. Introduction to Algorithms, Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein, PHI, 2009, Third Edition.

2. Fundamentals of Computer Algorithms, Ellis Horowitz, Sartaj Sahni and Sanguthevar Rajasekaran, Universities Press, 2011, Second Edition.
3. Algorithmic Graph Theory and Perfect Graphs, Martin Charles Golumbic, 2004, Elsevier, Second Edition.

Reference Books:

1. Treewidth: Computations and Approximations, Ton Kloks, Springer-Verlag, 1994.
2. Graph Classes A Survey : Andreas Brandstädt, Van Bang Le and Jeremy P.Spinard, SIAM, 1987.
3. Algorithms and Complexity, Herbert S. Wilf, AK Peters/CRC Press, 2002, Second Edition.
4. Parameterized Complexity, Rodney G. Downey and M. R. Fellows, Springer, 2012.
5. Approximation Algorithms, Vijay V. Vajirani, Springer, 2001.
6. Randomized Algorithms, Rajeev Motwani and Prabhakar Raghavan, Cambridge University Press, 1995.
7. Computers and Intractability: A Guide to the theory of NP-Incompleteness, Michael R. Garey and David S. Johnson, W.H. Freeman & Co., 1979, First Edition.
8. Topics in Domination in Graphs, Teresa W. Haynes, Stephen T. Hedetniemi and Michael A.Henning, Springer, 2020.

CS26003 **3-0-0 (3)**

Foundations of Cryptography

Pre-Requisites: **None**

Course Outcomes:

CO-1	Understand Number Theory and Algebra for design of cryptographic algorithms.
CO-2	Construct finite fields and apply number theoretic concepts in cryptographic algorithm.
CO-3	Analyse and compare symmetric-key encryption public-key encryption schemes based on different security models.
CO-4	Prove the security of cryptographic algorithms against attack models.
CO-5	Investigate and apply homomorphic encryption.

Course Articulation Matrix:

	PO-1	**PO-2**	**PO-3**	**PO-4**	**PO-5**	**PO-6**
CO-1	2		1	2	2	
CO-2	1				1	
CO-3	2		1	2	2	3
CO-4	2	1	2	3	3	3
CO-5	3	2	2	3	2	3

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Number Theory – Divisibility, Congruences, Quadratic residues and residuacity, Abstract Algebra – Groups, rings, fields, construction of finite fields, vector space, Galoise field cryptography- Notion and need for security proofs, Attack models, Perfect secrecy, Computational secrecy, One-time Pad (OTP), Pseudo-random generator (PRG), Pseudo- random function (PRF), design principles of stream and block ciphers, stream and block ciphers (DES, AES), Attacks on stream and block ciphers, Semantic security, Block cipher modes, Message Integrity – MAC and cryptographic hash function, NMAC, HMAC, Authenticated encryption.

One way function, Cryptographic hardness assumptions, Key exchange algorithms, Public key encryption algorithms (RSA, ElGamal, Rabin, ECC), Attacks on text book encryption algorithms, Semantically secure encryption algorithms, Security against chosen plain text and chosen cipher text attacks, Zero knowledge proofs, homomorphic encryption, Post quantum Cryptography.

Learning Resources:

Text Books:

1. N. Koblitz, Number Theory and Cryptography, Springer, 2001
2. J. Katz and Y. Lindell, Introduction to Modern Cryptography, Third edition CRC press, 2020.
3. Golreich O, Foundations of Cryptography, Vol.1.2, Cambridge University Press, 2004.

Reference books:

1. Wenbo Mao, Modern Cryptography: Theory and Practice, first edition, Pearson Education, 2004.
2. Menezes, et.al, Handbook of Applied Cryptography, CRC Press, 2004.

CS26005 **3-0-0 (3)**

Data Mining

Pre-Requisites: **None**

Course Outcomes:

CO-1	Analyze and evaluate performance of algorithms for frequent Itemsets.
CO-2	Analyze Classification algorithms.
CO-3	Analyze Clustering algorithms.
CO-4	Analyze Algorithms for sequential patterns.
CO-5	Determine patterns from time series data.

Course Articulation Matrix:

	PO-1	**PO-2**	**PO-3**	**PO-4**	**PO-5**	**PO-6**
CO-1	3	1	3	-	1	2
CO-2	3	1	3	-	1	2
CO-3	3	1	3	-	1	2
CO-4	3	1	3	-	1	2
CO-5	3	1	3	-	1	2

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Knowledge Discovery Process. Basic concepts of Association Rule Mining, Frequent Item set mining, Mining various kinds of association rules, Classification by decision tree induction, Bayesian Classification, Rule- based Classification, Classification Back-propagation, Clustering methods, Data Objects and Attribute Types, Basic Statistical Descriptions of Data, Measuring Data Similarity and Dissimilarity Partition based Clustering, Hierarchical based clustering, Density based clustering. Sequential Pattern Mining concepts, primitives, scalable methods; Transactional Patterns and other temporal based frequent patterns, Mining Time series Data, Periodicity Analysis for time related sequence data, Trend analysis, Similarity search in Time-series analysis

Learning Resources:

Text Books:

1. Jiawei Han and M Kamber, Data Mining Concepts and techniques, Morgan Kaufmann Publishers In, 2022; Fourth Edition.
2. Chris Chatfield, The Analysis of Time Series: An Introduction, Chapman & Hall/CRC, 2003, Sixth Edition.

Reference Books:

1. Pang-Ning Tan, Michael Steinbach, Anuj Karpatne and Vipin Kumar, Introduction to Data Mining, Pearson, 2018, Second Edition.
2. G. Dong and J Pei, Sequence Data Mining, Springer, 2007, First Edition.

CS26007 **0-0-3 (2)**

Cryptography Laboratory

Pre-Requisites: **None**

Course Outcomes:

CO-1	Implement and analyze the number theoretic algorithms.
CO-2	Assess attacks including brute force attacks on symmetric key encryption protocols
CO-3	Implement number theoretic algorithms using multi-precision integer package.
CO-4	Implement Public Key Cryptosystems and analyze their security.
CO-5	Implementation of Elliptic Curve Cryptosystem

Course Articulation Matrix:

	PO-1	**PO-2**	**PO-3**	**PO-4**	**PO-5**	**PO-6**
CO-1	1		1			
CO-2	3		2	1	1	1
CO-3	1		1			
CO-4	2		2	3	3	2
CO-5	2		1	3	2	2

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Programming Assignment Set 1:

a. Euclidean and Extended Euclidean algorithm for finding the Greatest Common Divisor of two large integers. Computing the Multiplicative inverses in Z_n.
b. Repeated square and multiply algorithm for modular exponentiation in *Zn.*
c. Determining the order of a group element. Finding a generator of a cyclic group.
d. Chinese remainder theorem.
e. Computation of Legendre symbol and Jacobi symbol
f. Modular polynomial arithmetic
g. RSA public key algorithm
h. ElGamal Cryptosystem
i. Rabin cryptosystem
j. Diffie-Hellman Key exchange protocol.

Programming Assignment Set II:

a. Pollard's rho algorithm for factoring integers.
b. Pollard's *p*-1 algorithm for factoring integers.
c. Fermat's factorization method

d. Congruence of squares. Finding a congruence of squares modulo *n* to factor *n*. e. Construction of Finite Field of characteristic 2.
e. Computations in elliptic curve over a finite field.

Programming Assignment Set III:

a. Sieve of Eratosthenes
b. Fermat primality test
c. Solovay-Strassen probabilistic primality test
d. Miller-Rabin probabilistic primality test
e. Lucas-Lehmer primality test

Instructions:

1. C/C++ Programming Language under Linux Operating System
2. gmp-man-6.1.2.pdf (Refer GMP library manual)
3. Code should be well modularised and documented
4. Use the standard coding style

Learning Resources:

Text Books:

1. Menezes, P.C. van Oorschot, S.A. Vanstone: Handbook of Applied Cryptography: CRC Press, 1996.

Reference Books

1. Abhijit Das and C.E.VeniMadhavan, *Public-key Cryptography: Theory and Practice*, Pearson, 2009.
2. Darrel Hankerson, Alfred Menezes, Scott Vanstone,*Guide to Elliptic Curve Cryptography*, Springer-Verlag, 2004.

CS26009 **0-0-3 (2)**

Data Mining Laboratory

Pre-Requisites: **None**

Course Outcomes:

CO-1	Implement algorithms for finding frequent Itemsets.
CO-2	Implement Classification algorithms.
CO-3	Implement Clustering algorithms.
CO-4	Develop programs for sequential patterns.
CO-5	Extract patterns from time series data.

Course Articulation Matrix:

	PO-1	**PO-2**	**PO-3**	**PO-4**	**PO-5**	**PO-6**
CO-1	3	1	3	-	1	2
CO-2	3	1	3	-	1	2
CO-3	3	1	3	-	1	2
CO-4	3	1	3	-	1	2
CO-5	3	1	3	-	1	2

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Implement Algorithms for finding frequent Itemsets and to generate association rules. Implement various Classification algorithms such decision tree construction, back-propagation algorithm on Feed forward ANNs. Implement partition based, hierarchical and density based Clustering algorithms. Design, develop and Implement algorithms for finding sequential patterns. Develop programs to extract patterns indicating trends in Time series Data. Perform periodicity analysis and do similarity search in time series data.

Learning Resources:

Text Books:

1. Jiawei Han and M Kamber, Data Mining Concepts and techniques, Morgan Kaufmann Publishers In, 2022; Fourth Edition.
2. Chris Chatfield, The Analysis of Time Series: An Introduction, Chapman & Hall/CRC, 2003, Sixth Edition.

Reference Books:

1. Pang-Ning Tan, Michael Steinbach, Anuj Karpatne and Vipin Kumar, Introduction to Data Mining, Pearson, 2018, Second Edition.
2. G. Dong and J Pei, Sequence Data Mining, Springer, 2007, First Edition.

2nd Semester

CS26002 **3-0-0 (3)**

Network Security

Pre-Requisites: CS26003

Course Outcomes:

CO-1	Design adversary models and protocols.
CO-2	Design of secure communication protocols in Internet applications.
CO-3	Analyze cryptographic algorithms.
CO-4	Identify security threats in Mobile Applications.
CO-5	Design of secure protocols for wireless ad-hoc and sensor networks.

Course Articulation Matrix:

	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1			1	2		2
CO-2			2	3		
CO-3				2		3
CO-4	2			2		2
CO-5				3		2

1 - Slightly; 2 - Moderately; 3 - Substantially

Syllabus:

Cryptographic algorithms, Pseudorandom Generators, Hash functions, Block ciphers, Stream Ciphers, Access Control Methods, Message Authentication and Digital Signatures, Design of secure Internet protocols, Key distributions, Design of Access control methods, Network Anomaly Detection methods, Mobile IPv6, https protocol, Design of Firewalls and Intrusion Detection Systems, Malware detection methods, Mobile application security models, Mobile threats and malware, Trust based protocols, Mobile app security, Vulnerabilities and Security Challenges in Wireless networks, Trust Assumptions, Adversary models and Protocols, Attacks against naming and addressing in the Internet, Security protocols for address resolution and address auto configuration, IP Security (IP Sec) protocol, Key Establishment and Revocation Protocols, Secure Neighbor Discovery, Secure routing protocols in multi-hop wireless networks, Provable Security for Ad-hoc Network routing protocols, Privacy preserving routing in Ad-hoc Networks, Location privacy in vehicular Ad-hoc networks.

Learning Resources:

Text Books:

1. John R. Vacca, *Computer and Information Security Handbook, Elsevier, 2009*
2. L. Buttyan, J. P. Hubaux, *Security and Cooperation in Wireless Networks,* Cambridge University Press, *2008.*

Reference Books:

1. *W. Trappe,* L. C. Washington, *Introduction to Cryptography with Coding Theory,* Prentice Hall 2005
2. Noureddine Boudriga, *Security of Mobile Communications,* Auerbach Publications, Taylor and Francis Group, 2010.

CS26004 **3-0-0 (3)**

Data Privacy

Pre-Requisites: **None**

Course Outcomes:

CO-1	Define differential privacy.
CO-2	Design techniques to achieve differential privacy for linear queries.
CO-3	Design mechanisms for query release problem using online learning algorithms.
CO-4	Analyze computational complexity of differentially private mechanisms.

Course Articulation Matrix:

	PO-1	**PO-2**	**PO-3**	**PO-4**	**PO-5**	**PO-6**
CO-1	2	2	2	2	2	2
CO-2	1	3	3	3	3	3
CO-3	1	2	3	3	3	3
CO-4	1	3	3	3	3	2

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

The Promise of Differential Privacy: Privacy-preserving data analysis; Basic Terms: The model of computation, Towards defining private data analysis, Formalizing differential privacy; Basic Techniques and Composition Theorems: Useful probabilistic tools, Randomized response, The laplace mechanism, The exponential mechanism, Composition theorems, The sparse vector technique; Releasing Linear Queries with Correlated Error: An offline algorithm: SmallDB, An online mechanism: private multiplicative weights; Generalizations: Mechanisms via α-nets, The iterative construction mechanism, Connections; Boosting for Queries: The boosting for queries algorithm, Base synopsis generators; When Worst-Case Sensitivity is Atypical: Subsample and aggregate, Propose test-Release, Stability and privacy; Lower Bounds and Separation Results: Reconstruction attacks, Lower bounds for differential privacy; Differential Privacy and Computational Complexity: Polynomial time curators, Some hard-to-Syntheticize distributions, Polynomial time adversaries; Differential Privacy and Mechanism Design: Differential privacy as a solution concept, Differential privacy as a tool in mechanism design, Mechanism design for privacy aware agents; Differential Privacy and Machine Learning: The sample complexity of differentially private machine learning, Differentially private online learning, Empirical risk minimization; Additional Models: The local model, Pan-private streaming model, Continual observation, Average case error for query release.

Learning Resources:

Text Books:

1. C. Dwork and A. Roth, *The Algorithmic Foundations of Differential Privacy*, now Publishers, 2014.

Reference Books:

1. Charu C. Aggarwal, *Privacy-Preserving Data Mining: Models and Algorithms*, 1st Edition Springer, 2008.
2. Relevant Research Papers

CS26006 **0-0-3 (2)**

Network Security Laboratory

Pre-Requisites: **None**

Course Outcomes:

CO-1	Develop secure traffic communication techniques in Internet applications.
CO-2	Analyze mobile threats and malwares.
CO-3	Design and Implement secure routing and medium access protocols in emerging Networks.

Course Articulation Matrix:

	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1				2		2
CO-2				2		2
CO-3				2		2

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Implementation of secure Internet protocols, Access control protocols, Network Anomaly Detection methods, Mobile IPv6, https protocol, Firewalls and Intrusion Detection Systems, Malware detection, Mobile application security models, Mobile threats and malware, Trust based protocols, Mobile web app security, Secure protocols for mobile adhoc networks, secure neighbor discovery, Wormhole detection mechanisms in wireless sensor networks, Secure routing in wireless adhoc and sensor networks, Secure MAC protocols

Learning Resources:

Text Books:

1. John R. Vacca, *Computer and Information Security Handbook, Elsevier, 2009*
2. L. Buttyan, J. P. Hubaux, *Security and Cooperation in Wireless Networks,* Cambridge University Press, *2008.*

Reference Books:

1. *W. Trappe,* L. C. Washington, *Introduction to Cryptography with Coding Theory,* Prentice Hall 2005
2. Noureddine Boudriga, *Security of Mobile Communications,* Auerbach Publications, Taylor and Francis Group, 2010.

CS26008 **0-0-3 (2)**

Data Privacy Laboratory

Pre-Requisites: **None**

Course Outcomes:

CO-1	Implementation of differential privacy mechanism for numeric, non-numeric and linear queries.
CO-2	Implement composition techniques in the design of mechanisms.
CO-3	Implement utility measurement of differential privacy to evaluate mechanisms.
CO-4	Classify the existing mechanisms into several types: transformation, partitioning of dataset, query separation and iteration.
CO-5	Build a system that supports that deferentially private data analysis.

Course Articulation Matrix:

	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	3	1	3	2	3	3
CO-2	3	1	3	1	3	3
CO-3	2	1	3	3	3	3
CO-4	2	1	2	2	3	3
CO-5	2	2	2	2	3	3

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

1. Implement differential privacy using the Laplace mechanism for numeric data
2. Implement differential privacy using the Exponential mechanism for non-numeric data
3. Implement differential privacy using the Gaussian mechanism for linear queries
4. Implement Sequential/parallel composition theorems in the design of the above mechanisms
5. Implement the utility measurements such as Noise size and error for data publishing and analysis to evaluate the performance of differential privacy mechanisms.
6. Use Machine learning approach to classify the mechanisms into several types

Learning Resources:

Text Books:

1. C. Dwork and A. Roth, The Algorithmic Foundations of Differential Privacy, now Publishers, 2014.

Reference Books:

1. Tianqing Zhu, Gang Li, Wanlei Zhou, Philip S. Yu, Differential Privacy and Applications, Springer International Publishing AG 2017.

CS26095 **0-0-0 (2)**

Minor Project

Pre-Requisites: **None**

Course Outcomes:

CO-1	Apply engineering principles to real-world projects
CO-2	Plan and monitor project tasks individually or as a team
CO-3	Demonstrate practical experience in project execution
CO-4	Communicate project findings clearly through reports and presentations

Course Articulation Matrix:

	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	3	3	3	3	3	
CO-2	2	2	2	2	2	
CO-3	2	2	2	2	2	
CO-4	1	1	1	1	1	

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Description:

Students are expected to choose real world or relevant problems and apply the engineering principles learned, to solve the problem through building prototypes or simulations or writing codes or establishing processes/synthesis/correlations etc. The department constituted panel can decide the suitability and worthiness of the project

Evaluation Criteria:

The student will be evaluated by the panel based on the below criteria. Weightage for each criterion will be determined by the panel and will be informed to the students.

Criteria	Description	Weightages
I	Identification of Problem Domain	15 Marks
II	Study of Existing Systems and establishing clear objectives	15 Marks
III	Planning of project and work distribution within the team	30 Marks
IV	Proper Documentation and Technical Writing	25 Marks
V	Presentation and Response to questions	25 Marks

Evaluation Criteria-CO Mapping

CO / Criteria	CO1	CO2	CO3	CO4
I	X			
II	X			
III		X	X	
IV				X
V				X

3rd Semester

CS26089 **0-0-0 (2)**

SEMINAR AND TECHNICAL WRITING

Pre-Requisites: **None**

Course Outcomes:

CO-1	Consolidate ideas based on expert talks attended.
CO-2	Prepare a well-organized report employing elements of critical thinking and technical writing.
CO-3	Demonstrate the ability to describe, interpret and analyze the subject matter and develop competence in presenting .

Course Articulation Matrix:

	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	2		2			3
CO-2	2		2			3
CO-3	2		2			3

1 - Slightly; 2 - Moderately; 3 - Substantially

Description:

In Seminar and Technical Writing, every student is expected to prepare a well-organized report based on one / all of the following:

- by attending at least 5 expert lectures/ invited talks/ Seminar/ Popular lectures etc. organized by the institute/any of the departments, ideally in a specific domain or with the same theme.
- prepare a business or marketing plan based on patent search

The student is expected to consolidate the ideas from these lectures/patent searches and may even include material from other sources to strengthen the content of the report. The student should prepare a well-organized report based on the above and present it to the panel constituted by the department, for evaluation.

Evaluation Criteria:

The student will be evaluated by the panel based on the below criteria.

Criteria	Description	Weightages
I	Clarity on the topic	15 Marks
II	List of lectures attended	15 Marks
III	Report	20 Marks
IV	Presentation	25 Marks
V	Response to questions	25 Marks

Evaluation Criteria-CO Mapping

CO / Criteria	CO1	CO2	CO3
I	X		
II	X		
III		X	
IV			X
V			X

CS26091 **0-0-0 (2)**

SHORT TERM INDUSTRIAL / RESEARCH EXPERIENCE

Pre-Requisites: **None**

Course Outcomes:

CO-1	Apply engineering principles to real-world problems, gaining practical experience
CO-2	Plan, manage and execute the work with ethical consideration
CO-3	Review the social and environmental impact of the work
CO-4	Communicate the learnings through report and presentation

Course Articulation Matrix:

	PO-1	PO-2	PO-3	PO-4	PO-5
CO-1	3	3	3	3	3
CO-2	2	2	2	2	2
CO-3					
CO-4					

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Description:

Every student has to undergo either a Summer Internship / Research project. The summer internship may be undergone in an Industry/Research organization or any premier academic Institution, including NIT Warangal for 6-8 weeks. The research project shall be registered under the guidance of any faculty member in the institute. The student is required to submit a report and present the work before an evaluation committee, nominated by the Head of the Department.

Evaluation Criteria:

The student will be evaluated by the panel based on the below criteria. Weightage for each criterion will be determined by the panel and will be informed to the students.

Criteria	Description	Weightages
I	Relevance of the area of work	10 Marks
II	Performance of the Task	25 Marks
III	Crucial learnings from the work	15 Marks
IV	Report Preparation	30 Marks
V	Presentation and Response to questions	20 Marks

Evaluation Criteria-CO Mapping

CO / Criteria	CO1	CO2	CO3	CO4
I	X			
II		X		
III			X	
IV				X
V				X

CS26093 **0-0-0 (2)**

COMPREHENSIVE VIVA-VOCE

Pre-Requisites: **None**

Course Outcomes:

CO-1	Comprehend the knowledge gained in the course work
CO-2	Demonstrate the ability in problem solving
CO-3	Communicate effectively using engineering terminology

Course Articulation Matrix:

	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	3	3	3	3		
CO-2	3	3	3	3		
CO-3	2	2	2	2		

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Description:

In Comprehensive viva-voce each student will be evaluated for their overall comprehension of the course work and laboratory training that they have undergone. The students will be expected to answer questions orally, write down simple equations, draw plots, schematics, write simple code etc. as questioned by the panel. Assessment will be done by the panel based on the student response.

CS26097 **0-0-0 (8)**

DISSERTATION: PART-A

Pre-Requisites: **None**

Course Outcomes:

CO-1	Identify a topic in advanced areas of Computer Science & Engineering.
CO-2	Review literature to identify gaps and define objectives and scope of the work.
CO-3	Employ the ideas from literature and develop research methodology.
CO-4	Develop a model, experimental set-up and / or computational techniques necessary to meet the objectives.

Course Articulation Matrix:

	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	3	2	3	1		3
CO-2	3	2	3	1		3
CO-3	3	3	3	3	3	3
CO-4	3	3	3	3	3	3

1 - Slightly; 2 - Moderately; 3 - Substantially

Description:

Students are expected to choose real-world contemporary problem and apply the engineering principles learned, to solve the problem through building prototypes or simulations or writing codes or establishing processes/synthesis/correlations etc. The department constituted panel will decide the suitability and worthiness of the project

Dissertation Evaluation:

i. The dissertation shall be submitted as per the schedule given in the academic calendar.

ii. The dissertation supervisor will periodically review the progress of the student and finally give his/her assessment of the work done by the student.

iii. The Dissertation Part – A will be evaluated for 100 marks, with the following weightages:

Sub-component	**Weightage**
a) Periodic evaluation by Guide	40 marks
b) Mid-term review	20 marks
c) End Semester viva-voce examination	40 marks

Evaluation Criteria

The student will be evaluated by the panel based on the below criteria. Weightage for each criterion will be determined by the panel and will be informed to the students.

Criteria	Description	Weightages
I	Selection of Topic	10 Marks
II	Literature Survey	15 Marks
III	Defining the Objectives and Solution Methodology	25 Marks
IV	Performance of the Task	50 Marks

Evaluation Criteria - CO Mapping:

CO / Criteria	CO1	CO2	CO3	CO4
I	X			
II		X		
III			X	
IV				X

Refer to MTech. – Regulations for any further information regarding Mid-term review, End Sem evaluation, Template for report preparation and plagiarism”

4th Semester

CS26098 **0-0-0 (12)**

DISSERTATION: PART-B

Pre-Requisites: **CS26097**

Course Outcomes:

CO-1	Identify the materials and methods for carrying out experiments/develop a code.
CO-2	Execute the research methodology with a concern for society, environment and ethics
CO-3	Analyze, discuss and justify the results/trends and draw valid conclusions.
CO-4	Prepare the report as per recommended format and present the work orally adhering to stipulated time.
CO-5	Explore the possibility to publish/present a paper in peer reviewed journals/conference proceedings without plagiarism.

Course Articulation Matrix:

	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	2		3	3	2	3
CO-2	2		3	3	2	3
CO-3	3		3	3	2	3
CO-4	3	3	3	3	3	3
CO-5	3	3	3			3

1 - Slightly; 2 - Moderately; 3 - Substantially

Description:

Students are expected to choose real-world contemporary problem and apply the engineering principles learned, to solve the problem through building prototypes or simulations or writing codes or establishing processes/synthesis/correlations etc. The department constituted panel will decide the suitability and worthiness of the project.

Evaluation Criteria:

The student will be evaluated by the panel based on the below criteria as a continuation of Dissertation Part A. Weightage for each criterion will be determined by the panel and will be informed to the students.

Task	Description	Weightages
IV	Performance of the Task	15 Marks
V	Dissertation Preparation	15 Marks
VI	Review (Presentation & Understanding)	20 Marks
VII	Viva-Voce	40 Marks
VIII	Publications /Possibility of publication	10 Marks

Evaluation Criteria-CO Mapping:

CO / Criteria	CO1	CO2	CO3	CO4	CO5
IV	X	X			
V				X	
VI			X		
VII				X	
VIII					X

Refer to M.Tech. – Regulations for any further information regarding Mid-term review, End Sem evaluation, Template for report preparation and plagiarism".

Professional Elective-I/II Courses

CS26021 **3-0-0 (3)**

Biometric Security

Pre-Requisites: **None**

Course Outcomes:

CO-1	Analyse biometric systems.
CO-2	Design basic biometric system applications.
CO-3	Identify the acceptance issues associated with the design and implementation of biometric systems.
CO-4	Identify various Biometric security issues.
CO-5	Design biometric system to solve security issues.

Course Articulation Matrix:

	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	1					3
CO-2		1				2
CO-3	1		1		2	
CO-4	1			1		
CO-5					1	1

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Person Recognition, Biometric Sytems, Biometric Functionalities, Biometric System Errors, Design cycle of Biometric Systems, Applications of Biometric Systems, Security and Privacy issues, Fingerprint recognition, friction and ridge pattern, fingerprint acquisition, sensing techniques, feature extraction, ridge orientation and frequency estimation, singularity extraction, minutiae extraction, matching, fingerprint indexing, synthesis, palmprint recognition, Face recognition sensors, cameras, Video sequences, Viola Jones face detection, appearance based , model based, texture based face recognition, Principal Component Analysis, Linear Discriminant Analysis, Independent Component Analysis, Heterogeneous face recognition, Iris Recognition, Design, segmentation, normalization, encoding and matching, quality, Additional biometric traits, Ear, Gait, Hand geometry, soft biometrics, multibiometrics, multi-sensor, multi-algorithm, multi-instance, multi-sample, multi-modal systems, processing architectures, processing sequence, sensor level, feature level, score level, rank level, and decision level fusion, Attacks on biometric systems, adversary attacks, user interface, processing, template databases.

Learning Resources:

Text Books:

1. Anil K. Jain, Arun A. Ross, Karthik Nandakumar, Introduction to biometrics, Springer, 2011

2. Anil K Jain, Patrick Flynn and Arun A Ross, *Handbook of Biometrics*, Springer,USA,2010.

Reference books

1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi, *Biometrics -Identity verification in a network*, 1st Edition, Wiley Eastern, 2002.

2. John Chirillo, Scott Blaul, *Implementing Biometric Security*, 1st Edition, Wiley Eastern Publication, 2005.
3. John R Vacca, *Biometric Technologies and Verification Systems*, Elsevier, USA, 2007.
4. Paul Reid, *Biometrics for Network Security*, Pearson Education, New Delhi, 2004.
5. David D Zhang, *Automated Biometrics: Technologies and Systems*, Kluwer Academic Publishers, New Delhi, 2000.

CS26023 **3-0-0 (3)**

Computability and Complexity

Pre-Requisites: **None**

Course Outcomes:

CO-1	Understand the limits of models of computation under the Church-Turing hypothesis.
CO-2	Classify problems into appropriate complexity classes.
CO-3	Identify the possibility of intractability for a given problem.
CO-4	Apply the concept of interactive proofs in the analysis of optimization problems.

Course Articulation Matrix:

	PO-1	**PO-2**	**PO-3**	**PO-4**	**PO-5**	**PO-6**
CO-1	1			1		
CO-2	1					1
CO-3				1		1
CO-4	1		1	2		1

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Computability: Models of computation, The Church–Turing Thesis, Turing model of computation, Variants of Turing machines, Decidable, semi-decidable and undecidable problems, Post correspondence problem, Mapping reducibility, The recursion theorem, The Rice's theorem, Decidability of logical theories and Turing reducibility.

Complexity: Introduction to complexity theory, Nondeterminism and NP-completeness, Diagonalization, Relations between the standard complexity classes, The Cook–Levin theorem, Space complexity, Savitch's theorem, PSPACE, PSPACE-completeness ,Circuits, Randomized computation and complexity, Interactive proof systems, Complexity of counting, Parallel computation and complexity, Probabilistic complexity classes, Decision trees, Communication complexity , Circuit complexity, Probabilistically checkable proofs, Quantum computation and Logic in complexity theory.

Learning Resources:

Text Books:

1. Christos H. Papadimitriou, *Computational Complexity*, Addison-Wesley, 1994.
2. Michael Sipser, *Introduction to Theory of Computation*, Third edition, PWS Publishing Company, 2012.

Reference books

1. Sanjeev Arora and Boaz Barak ,*Computational Complexity: A Modern Approach*, Cambridge University Press, 2010.

CS26025 **3-0-0 (3)**

Digital Video Processing

Pre-Requisites: **None**

Course Outcomes:

CO-1	Use the suitable image/video acquisition approach, representation and quality assessment for a given scenario.
CO-2	Apply image/video processing operations for enhancement and restoration.
CO-3	Understand image/video compression standards.
CO-4	Solve a video indexing, summarization, browsing and retrieval problem.
CO-5	Implement an approach to solve a video analytics problem.

Course Articulation Matrix:

	PO-1	**PO-2**	**PO-3**	**PO-4**	**PO-5**	**PO-6**
CO-1	1	2	1			
CO-2	2	2				
CO-3	-	2	1			
CO-4	3	2	1			1
CO-5	3	2	1		1	1

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Introduction – Introduction to digital image and video processing.

Image/Video processing – Intensity transformations, Applications of linear filtering and non linear filtering. Morphological operations. Colour image processing. Features for Image and Video processing. Geometric transforms and Image registrations, Image segmentation and analysis. Spatiotemporal noise filtering, coding artifact reduction, Blotch detection and removal, video stabilization, and recent image/video operations and features in contemporary literature.

Image Compression – lossless coding, block transform coding, fundamentals of vector quantization, wavelet image compression, JPEG image compression.

Video Compression – basic concepts and techniques of video coding and the H.261 Standard, spatiotemporal subband/Wavelet Video Compression, Object-based video coding, introduction to video coding standards and formats: H.261, MPEG-2/DVB, MPEG-4, H.264/AVC, H.265/HEVC, H.266/VVC.

Image and Video Acquisition – Image scanning, sampling and interpolation, video sampling and interpolation. Recent standards and practices in image and video acquisition.

Video Quality Assessment – Introduction, HVS Modelling based methods, feature based methods, motion modelling-based methods, and approaches based on contemporary research.

Indexing, Summarization, Browsing and Retrieval – Introduction, Image and Video features, Video analysis, video representation, video browsing and video retrieval. Video features in contemporary research.

Video Analytics – Review of video analytics algorithms for: motion and change detection, object detection, object tracking, behaviour analysis, face recognition, Image and Video classification and recent visual analytics approaches in contemporary research.

Learning Resources:

Text Books:

1. Alan C. Bovik, The Essential Guide to Video Processing, Academic Press, 2009, 2nd Edition
2. Alan C. Bovik, Handbook of Image and Video Processing, Academic Press, 2005, 2nd Edition
3. Shengrong Gong, Chunping Liu, Yi Ji, Baojiang Zhong, Yonggang Li, Husheng Dong, Advanced Image and Video Processing Using MATLAB, Springer, 2019.
4. Vaibhav Verdhan, Computer Vision Using Deep Learning Neural Network Architectures with Python and Keras, Apress, 2021

Reference Books:

1. A. Murat Tekalp, Digital Video Processing, Pearson, 2015, 2nd Edition
2. Richard Szeliski, Computer Vision: Algorithms and Applications, Springer, 2022, 2nd Edition
3. David Bull, Fan Zhang, Intelligent Image and Video Compression: Communicating Pictures, Academic Press, 2021, 2nd Edition

CS26027 **3-0-0 (3)**

Cryptanalysis

Pre-Requisites: **None**

Course Outcomes:

CO-1	Analysis of vulnerabilities in an elliptic curve cryptography.
CO-2	Identify security vulnerabilities of different types of cryptosystems.
CO-3	Analyze methods of attacking symmetric key cryptography.
CO-4	Analyze methods of public key cryptography.
CO-5	Development of secure cryptosystem.

Course Articulation Matrix:

	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	1		1	2		1
CO-2	1		1	2		2
CO-3	1		1	2		1
CO-4	1		1	2		1
CO-5	2		2	3	2	2

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Modern Cryptography Preliminaries - Defining security in cryptography, Number theory concepts Linear Algebra, Sieving methods, Tutorial, Introduction to symmetric key cryptography, Symmetric ciphers- triple DES, Modes of operation, Stream ciphers –RC4, Stream ciphers – Attacks, Linear analysis. Differential analysis, Tutorials, Introduction to public key cryptography, Public key cryptography and RSA. Key management and Distribution, Other public Key Cryptosystems, Attacks on RSA, Attacks on Diffie-Hellman Attacks on ElGamal. Introduction to Discrete Logarithm Problem. Shanks baby step and Gaint step algorithm, Pollard Rho, Pollard Kangaroo, Pohlig-Hellman. Introduction to index calculus method, Number Field Sieve method, Introduction to Elliptic Curve Cryptography, Generic algorithms to solve ECDLP, Anomalous attack, MOV attack.

Learning Resources:

Text Books:

1. Antoine Joux, Algorithmic Cryptanalysis, CRC Press, 2009
2. Gregory V. Bard, Algebraic Cryptanalysis, Springer, 2009

Reference Books

1. I. Blake, G.Seroussi and N.Smart, Elliptic Curves in Cryptography, Cambridge University Press, 1999.

2. I. Blake, G.Seroussi and N.Smart, Advances in Elliptic Curve Cryptography, Cambridge University Press, 2005.

3. Victor Shoup, A Computational Introduction to Number Theory and Algebra,II Edition, Cambridge University Press, 2008

4. Arjen K. Lenstra and Hendrik W. Lenstra, The Development of the Number Field Sieve, Lecture notes in Mathematics, Springer Berlin, Heidelberg, 1993.

CS26029 **3-0-0 (3)**

Information Security and Secure Coding

Pre-Requisites: **None**

Course Outcomes:

CO-1	Analyse and understand secure design.
CO-2	Analyse and apply authentication and authorization principles.
CO-3	Design secure application.
CO-4	Writing secure software.

Course Articulation Matrix:

	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	2	2	2	3	3	3
CO-2	1	1	3	2	2	2
CO-3	3	2	2	3	3	3
CO-4	1	3	1	1	1	2

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Information Security Basics: Introduction to Information Security – Risk Analysis – Legal Issues – Secure Design – Policy, Standards, Procedures and Guidelines – Security Organization structure; **Information Security Policy and Compliance:** Authentication and Authorization principles - Securing unstructured data – Information Rights Management – Storage security – Data base security; **Secure Application:** Secure application design – Writing Secure Software – J2EE vulnerabilities; **Secure Infrastructure Management:** Security Operations Management – Disaster Recovery and Backups – Physical Security.

Learning Resources:

Text Books:

1. Information Security – The complete reference; Chapters: 1-9, 11-12, 26-28, 31, 32, and 34 Author: Mark Rhodes – Ousley; McGraw Hill, 2013;ISBN Number: 978-0-07-178436-8

Reference Books

1. Whitman, Michael E., and Herbert J. Mattord. Principles of information security. Boston, MA: Thomson Course Technology, 2009.

CS26031 **3-0-0 (3)**

Information Systems Control and Auditing

Pre-Requisites: **None**

Course Outcomes:

CO-1	Ability to recognize the propensity of errors and remedies in processes involving Information Technology.
CO-2	A consummate knowledge of risks and controls in IT operations in Industry.
CO-3	An ability to provide protective IT security guidelines for various types of Industries.
CO-4	The necessary wherewithal to become an IS Auditor and/or Security specialist eventually.
CO-5	Evaluate asset safeguarding and data integrity, system effectiveness and system efficiency.

Course Articulation Matrix:

	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	1		2			2
CO-2	1	1	1	1	1	1
CO-3			1			1
CO-4			2			
CO-5			2			1

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Introduction: Overview of Information Systems Auditing. Conducting an Information Systems Audit. Management and the application Control Framework: Top Management Controls, Security Management Controls. Operations Management Controls. Quality Assurance Management Controls. Boundary Controls. Communication Controls.

Evidence Collection and Evidence evaluation: Audit Software. Concurrent Auditing Techniques. Interviews, Questionnaires, and Control Flowcharts. Evaluating Asset Safeguarding and Data Integrity. Evaluating System Effectiveness and System Efficiency. Managing the Information Systems Audit Function.

Practice study: CISA examination questions.

Learning Resources:

Text Books:

1. Ron Weber, *Information Systems Control and Audit*, Pearson Education, 1999
2. John B. Kramerk, *The CISA Prep Guide*, Wiley Publications, 2003 *3. Information Systems Control and Audit*, BOS, Institute of Chartered Accountants of India, New Delhi, 2013

Reference Books

1. Otero, Angel R. *Information technology control and audit*. Auerbach Publications, 2018.

CS26033 **3-0-0 (3)**

Mathematical Models for Internet

Pre-Requisites: **None**

Course Outcomes:

CO-1	Illustrate TCP/IP protocol stack including IPv4 and IPv6.
CO-2	Analysis of network (Internet) Traffic using queuing disciplines.
CO-3	Analysis of congestion control algorithms by considering network throughput and delay.
CO-4	Design of routing algorithms for the Internet.

Course Articulation Matrix:

	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	1			1		
CO-2	1			1	1	1
CO-3	1			1	1	2
CO-4	2			1	2	2

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Introduction to Internet and TCP/IP protocol stack, IPv4 and IPv6, Stochastic Processes (The Poisson process and Markov chains), Analysis of network (Internet) Traffic using queuing disciplines (M/M/1, M/M/1/C and M/M/C/C), Randomized algorithms and File sharing in the Internet, Networks and Graphs (including the internet graph and web graph), Analysis of Algorithms for Congestion Control, Performance Analysis of TCP Reno, TCP Tahoe and TCP Vegas, Linear Analysis with Delay: The single link case, Linear Analysis with Delay: The network case, Routing protocols for next generation Internet traffic, Mathematical models for Internet of Things.

Learning Resources:

Text Books:

1. FabrizioLuccio, Linda Pagli and Graham Steel, *Mathematical and Algorithm Foundations of the Internet*, Chaman and Hall, 2011
2. D. Bertsekas and R. Gallagar, *Data Networks*, PHI, 2nd Edition, 1992

Reference Books:

1. RayadurgamSrikant, *The Mathematics of Internet congestion control (systems and control: foundations and applications)*, 1st Edition, Birkhauser, 2003.
2. S. M. Ross, *Stochastic Processes*, Wiley, 2nd Edition, 1996

CS26035 **3-0-0 (3)**

Probabilistic Algorithms

Pre-Requisites: **None**

Course Outcomes:

CO-1	Design and analyze efficient randomized algorithms.
CO-2	Apply tail inequalities to bound error-probability.
CO-3	Analyze randomized algorithms with respect to probability of error and expected running time.
CO-4	Apply probabilistic method to demonstrate existence of combinatorial objects.
CO-5	Apply to graph problems.

Course Articulation Matrix:

	PO-1	**PO-2**	**PO-3**	**PO-4**	**PO-5**	**PO-6**
CO-1	2	1	1	2	1	2
CO-2				1		
CO-3	1			1	2	2
CO-4	1	1	1	1	1	1
CO-5	1	1	1		1	

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Las Vegas and Monte Carlo Algorithms, Computational Model and Complexity Classes, Game Tree Evaluation, The Markov and Chebyshev Inequalities, The Stable Marriage Problem, The Coupon Collectors Problem, The Chernoff Bound, Routing in a Parallel Computer, The Probabilistic Method: Overview, probabilistic analysis, use of indicator random variables, Randomly permuting arrays, Birthday paradox, analysis using indicator random variables, Balls and bins, Streaks, Online hiring problem, Maximum Satisfiability, Expanding Graphs, The Lovasz Local Lemma, Markov Chains, Random Walks on Graphs, Graph Connectivity, Expanders and Rapidly Mixing Random Walks, Pattern Matching, Random Traps, Skip Lists, Hash Tables, Linear Programming, The Min-Cut Problem, Minimum Spanning Trees, The DNF Counting Problem, The Online approximations paging Problem, Adversary Models and Paging against an Oblivious Adversary, Randomized number theoretic and algebraic algorithms.

Learning Resources:

Text Books:

1. Rajeev Motwani, PrabhakarRaghavan, *Randomized Algorithms*, Cambridge University Press, 1995.

Reference Books:

1. J. Hromkovic, *Design and Analysis of Randomized Algorithms*, Springer 2005.

CS26037 **3-0-0 (3)**

Secure Cloud Computing

Pre-Requisites: **None**

Course Outcomes:

CO-1	Analyze the security and privacy issues in the cloud computing.
CO-2	Understand the auditing and compliance process.
CO-3	Build security as a cloud service for secure cloud computing.
CO-4	Implement various case studies.
CO-5	Analyze the security and privacy issues in the cloud computing.

Course Articulation Matrix:

	PO-1	**PO-2**	**PO-3**	**PO-4**	**PO-5**	**PO-6**
CO-1	1		1	2	2	1
CO-2	1			1	2	2
CO-3			1	2	2	2
CO-4				2	1	2
CO-5			1	1	1	1

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Introduction to cloud computing; Infrastructure security; Data security and storage; Identity and access management; Security management in the cloud; Privacy; Audit and compliance; Example of cloud service providers – Amazon web services, Google, Microsoft Azure service platform; Security-as-a-(cloud) service; The impact of cloud computing on the role of corporate IT; The future of the cloud

Learning Resources:

Text Books:

1. Tim Mather, Subra Kumaraswamy and Shahed Latif, Cloud Security and Privacy, O'Reilly, 2009

Reference Books:

1. Rajkumar Buyya, Christian Vecchiola and S. Thamarai Selvi, Mastering Cloud Computing: Foundations and Applications Programming, Morgan Kaufmann, 2013
2. Barrie Sosinsky, Cloud Computing Bible, Wiley Publishing, 2011

Other Suggested Readings:

1. NPTEL Course on Cloud Computing by Prof. Soumya Kanti Ghosh, IIT Kharagpur, Prof. Rajiv Mishra, IIT Patna, Prof. Bidisha Chaudhuri, Prof. Amit Prakash, IIIT Bangalore

CS26039 **3-0-0 (3)**

Secure Software Engineering

Pre-Requisites: **None**

Course Outcomes:

CO-1	Evaluate secure software engineering problems, including the specification, design, implementation, and testing of software systems.
CO-2	Elicit, analyze and specify security requirements through SRS.
CO-3	Design and Plan software solutions to security problems using various paradigms.
CO-4	Model the secure software systems using Unified Modeling Language Sec(UMLSec).
CO-5	Develop and apply testing strategies for Secure software applications.

Course Articulation Matrix:

	PO-1	**PO-2**	**PO-3**	**PO-4**	**PO-5**	**PO-6**
CO-1	2		2	1		2
CO-2	2	2	1	1		2
CO-3	2		2	1		2
CO-4	1	1	1	1		1
CO-5	2		2	1		2

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Software assurance and software security, threats to software security, sources of software insecurity, benefits of detecting software security, managing secure software development, Defining properties of secure software, how to influence the security properties of software, how to assert and specify desired security properties, Secure software Architecture and Design: Software security practices for architecture and design: Architectural risk analysis, software security knowledge for Architecture and Design: security principles, security guidelines, and attack patterns, secure design through threat modeling, Writing secure software code: Secure coding techniques, Secure Programming: Data validation, Secure Programming: Using Cryptography Securely, Creating a Software Security Programs. Secure Coding and Testing: code analysis- source code review, coding practices, static analysis, software security testing, security testing consideration through SDLC

Learning Resources:

Text Books:

1. Julia H Allen, Sean J Barnum, Robert J Ellison, Gary McGraw, Nancy R Mead, *Software Security Engineering: A Guide for Project Managers*, Addison Wesley, 2008
2. Ross J Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd Edition, Wiley, 2008.

Reference Books:

1. Howard, M. and LeBlanc, D., *Writing Secure Code*, 2nd Edition, Microsoft Press, 2003.

CS26041 **3-0-0 (3)**

Unix Internals

Pre-Requisites: **None**

Course Outcomes:

CO-1	Design and implement Unix kernel data structures and algorithms.
CO-2	Analyze synchronization problems in uniprocessor and multiprocessor systems.
CO-3	Evaluate the scheduling requirements of different types of processes and find their solutions.
CO-4	Implement user level thread library and mimic the behaviour of Unix kernel for scheduling, synchronization and signals.

Course Articulation Matrix:

	PO-1	**PO-2**	**PO-3**	**PO-4**	**PO-5**	**PO-6**
CO-1	2		1	1	3	
CO-2				2	3	1
CO-3				2	3	1
CO-4	1		2	2	3	1

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Introduction to UNIX, The process and the kernel, Mode, space and context, Process abstraction, executing in kernel mode, synchronization by blocking interrupts, process scheduling. Introduction to Threads: Fundamental abstractions, Lightweight process design, issues to consider, User level thread libraries, scheduler activations, Multi-threading on Solaris, Pthreads library, Thread library implementation Using ucontext_t structures. Signals: Signal generation and handling, Unreliable signals, Reliable signals, Signals in SVR4, Signals implementation, Exceptions, Process Groups. Process Scheduling: Clock interrupt handling, Scheduler Goals, Traditional UNIX scheduling, Scheduling case studies. Synchronization and Multiprocessing: Introduction, Synchronization in Traditional UNIX Kernels, Multiprocessor Systems, Multiprocessor synchronization issues, Semaphores, spin locks, condition variables Read-write locks for multiprocessor systems, Reference counts and other considerations. Kernel Memory Allocators: Resource map allocator, Simple power of-two allocator, McCusick-Karels Allocator, Buddy system, SVR4 Lazy Buddy allocator, OSF/1 Zone Allocator, Hierarchical Allocator, Solaris Slab Allocator. File system interface and framework: The user interface to files, File systems, Special files, File system framework, The Vnode/Vfs architecture, Implementation Overview, File System dependent objects, Mounting a file system, Operations on files. File System Implementations : System V file system (s5fs) implementation, Berkeley FFS, FFS functionality enhancements and analysis, Temporary file systems, Buffer cache and other special-purpose file systems.

Learning Resources:

Text Books:

1. UreshVahalia, *UNIX Internals*, Pearson Education, 2005.

2. Richard Stevens, Stephen Rago, *Advanced Programming in the UNIX Environment*, Pearson Education, 2/e, 20056. Paul Reid, *Biometrics for Network Security*, Pearson Education, New Delhi, 2004.

Reference Books:

1. David D Zhang, *Automated Biometrics: Technologies and Systems*, Kluwer Academic Publishers, New Delhi, 2000.

CS26043 **3-0-0 (3)**

Web and Database Security

Pre-Requisites: **None**

Course Outcomes:

CO-1	Identify access control methods for secure web & database application development.
CO-2	Analyse vulnerabilities in the Web and Database applications.
CO-3	Design & Evaluate methods for web & database intrusion detection.
CO-4	Apply security audit methods.
CO-5	Design Secure Database schema.

Course Articulation Matrix:

	PO-1	**PO-2**	**PO-3**	**PO-4**	**PO-5**	**PO-6**
CO-1	1	1	1	1	1	1
CO-2		1	1	1	1	1
CO-3		1	2	2	1	2
CO-4						2
CO-5	1		2	2		1

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Database Basics: Overview of Relational Model, SQL, Building of database, Manipulation of data; Goals of Database Security, access points of database security, database security levels, and menaces to databases. Database security methods and methodologies, Security controls: flow control, inference control and access control, Database Application Security models – Types of users, access matrix model, access modes model, commonly used application types. Classes of access control: Discretionary access control (DAC), Mandatory access control (MAC) and Role based Access control (RBAC); Discretionary Access Control (DAC) mechanisms such as capabilities, profiles, access control lists, passwords, and permission bits. RBAC based security models features like User role assignment, Support for role relationships and Constraints , Assignable privileges. MAC based security models. Implementing Fine Grained access controls with views , Virtual Private databases: need for VPDs, Implementing VPD using views, The Database Security Design includes the controls that will be implemented to restrict users from accessing information, based on how the information is classified and the security model. HTML Injection and Cross- Site Scripting, Cross-Site Request, Forgery, SQL Injection and Data Store Manipulation, Breaking Authentication Schemes, Abusing Design Deficiencies, Leveraging Platform Weaknesses, Statistical database security; Database privacy – Hippocratic databases

Text Books:

1. Mike Shema, Hacking Web Apps Detecting and Preventing Web Application Security Problems, Syngress publications- Elsevier, 2012
2. M. Gertz, S. Jajodia, Handbook of Database Security, Springer, 2008.

Reference Books:

1. A Ben-Natan, R. B., Implementing Database Security and Auditing: Includes Examples for Oracle, SQL Server, Db2 Udb, Sybase, Digital Press, 2005
2. SilvanoCastano, Fugini, Martella, Samarati, Database Security, Addison Wesley, 1994.

Professional Elective-III/IV/V Courses

CS26022 **3-0-0 (3)**

Algorithmic Coding Theory

Pre-Requisites: None

Course Outcomes:

CO1	Understand Shannon's noisy coding theorem, Shannon capacity, and entropy.
CO2	Design of error-correcting codes and decoding algorithms.
CO3	Design and Analysis of lightweight and code-based cryptosystems.
CO4	Design of network coding algorithms for communication networks.

Course Articulation Matrix:

	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	2	_	2	_	_	_
CO-2	3	_	2	2	2	3
CO-3	2	_	2	3	2	3
CO-4	3	_	2	3	2	3

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Shannon Theorem, Shannon capacity, Hamming's Theory, Error correcting codes, Linear codes, Impossibility results for codes, Mac Williams Identities, Linear programming bound, The asymptotic perspective, Encoding, Decoding from erasures, Decoding RS codes, List decoding, linear time decoding, LDPC codes, Sipser-Spielman codes, Linear time encoding and decoding, Linear time and near optimal error decoding, Expander based constructions of efficiently, decodable codes, Some NP hard coding theoretic problems, Applications in complexity theory, Cryptography with error correcting codes, Lossless Multicast Network Coding, Network coding in Lossy Networks, Security against adversarial errors, Error correction bounds for centralized network coding.

Learning Resources:

Text Books:

1. Tom Richardson, RudigerUrbanke, Modern Coding Theory, Cambridge University Press, 2008
2. John b. Anderson and Seshadri Mohan, Source and Channel Coding: An Algorithm Approach, Springer, 1991.
3. G. Kabatiansky, E. Krouk and S. Semenov, *Error Correcting Coding and Security for Data Networks,* John Wiley & Sons Ltd., 2005.

Reference Books:

1. Jiri Adamek, Foundations *of* Coding, Wiley Interscience Publication, John Wiley & Sons, 1991

CS26024 **3-0-0 (3)**

Cyber crime and Information Warfare

Pre-Requisites: **None**

Course Outcomes:

CO-1	Understand principles of cyber crime and cyber forensics.
CO-2	Verify cryptography techniques using Cryptool.
CO-3	Apply appropriate countermeasures to defend threats.
CO-4	Apply suitable forensic tools for forensic analysis.
CO-5	Understand social and web intelligence in era of information age.

Course Articulation Matrix:

	PO-1	**PO-2**	**PO-3**	**PO-4**	**PO-5**	**PO-6**
CO-1	1					
CO-2				1		1
CO-3	1		1	2	1	2
CO-4	1		1	2	1	2
CO-5	2		2	2		2

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

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 perception management.

Defenses: Countermeasures including authentication, encryption, auditing, monitoring, intrusion detection, and firewalls, and the limitations of those countermeasures. Introduction to Open Source Intelligence (OSINIT), web intelligence and social media intelligence. Cyberspace law and law enforcement, information warfare and the military, and intelligence in the information age.

Learning Resources:

Text Books:

1. Information Warfare, Ventre, John Wiley & Sons, 15-Feb-2016

2. J. Wiles and A.Reyes, The Best Damn Cybercrime and Digital Forensics Book Period, Syngress, 2007.

Reference Books:

1. Grabosky, Peter. Cyber crime and information warfare. Australian Institute of Criminology, 2000.
2. Britz, Marjie. Computer forensics and cyber crime: An introduction, 2/e. Pearson Education India, 2009.

CS26026 **3-0-0 (3)**

Cyber Laws and Intellectual Property Rights

Pre-Requisites: **None**

Course Outcomes:

CO-1	Understand cyberspace, issues there in and need for a cyber law.
CO-2	Understand facets of India IT act n addressing e-trade and e-governance.
CO-3	Understanding of issues and problems arising out of online transactions.
CO-4	Understanding crimes with case law.
CO-5	Understand of intellectual property issues and development of the law in this regard.

Course Articulation Matrix:

	PO-1	**PO-2**	**PO-3**	**PO-4**	**PO-5**	**PO-6**
CO-1		2	1	1		2
CO-2		2	1			2
CO-3		2	1	1		2
CO-4		2	2			2
CO-5		2	1	1		2

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Cyber Space- Fundamental definitions -Interface of Technology and Law – Jurisprudence and-Jurisdiction in Cyber Space - Indian Context of Jurisdiction -Enforcement agencies – Need for IT act - UNCITRAL – E- Commerce basics; Information Technology Act, 2000 - Aims and Objects — Overview of the Act – Jurisdiction -Electronic; Governance – Legal Recognition of Electronic Records and Electronic Evidence - Digital Signature Certificates - Securing Electronic records and secure digital signatures - Duties of Subscribers - Role of Certifying Authorities - Regulators under the Act -The Cyber Regulations Appellate Tribunal - Internet Service Providers and their Liability– Powers of Police under the Act – Impact of the Act on other Laws; Cyber Crimes -Meaning of Cyber Crimes –Different Kinds of Cyber crimes – Cyber crimes under IPC; Cr.P.C and Indian Evidence Law - Cyber crimes under the Information Technology Act,2000 - Cyber crimes under International Law - Hacking Child Pornography, Cyber Stalking, Denial of service Attack, Virus Dissemination, Software Piracy, Internet Relay Chat (IRC) Crime, Credit Card Fraud, Net Extortion, Phishing etc - Cyber Terrorism- Violation of Privacy on Internet - Data Protection and Privacy – Indian Court cases; Intellectual Property Rights – Copyrights- Software – Copyrights vs Patents debate - Authorship and Assignment Issues - Copyright in Internet - Multimedia and Copyright issues - Software Piracy - Trademarks - Trademarks in Internet – Copyright and Trademark cases, Patents - Understanding Patents - European Position on Computer related Patents, Legal position on Computer related Patents - Indian Position on Patents – Case Law, Domain names - registration - Domain Name Disputes-Cyber Squatting-IPR cases

Learning Resources:

Text Books:

1. Justice Yatindra Singh, *Cyber Laws*, Universal Law Publishing Co., New Delhi, 2010
2. Farooq Ahmed, *Cyber Law in India,* New Era publications, New Delhi, 2005
3. S.R.Myneni, *Information Technology Law(Cyber Laws),* Asia Law House, Hyderabad, 2014

Reference Books:

1. Chris Reed, *Internet Law-Text and Materials*, Cambridge University Press, 2004
2. Pavan Duggal, *Cyber Law- the Indian perspective,* Universal Law Publishing Co., New Delhi, 2004

CS26028 **3-0-0 (3)**

Cyber Security

Pre-Requisites: **None**

Course Outcomes:

CO-1	Understand the cyber security fundamentals.
CO-2	Identify & Evaluate cyber security threats and vulnerabilities in Information Systems and apply security measures to real time scenarios.
CO-3	Design and implement appropriate security techniques and cyber policies to protect computers and digital information.
CO-4	Identify common trade-offs and compromises that are made in the design and development process of Information Systems.
CO-5	Demonstrate the use of standards and cyber laws to enhance information security in the development process and infrastructure protection.

Course Articulation Matrix:

	PO-1	**PO-2**	**PO-3**	**PO-4**	**PO-5**	**PO-6**
CO-1			1			1
CO-2	2		2	2		2
CO-3	2		2	2		2
CO-4	1			1		
CO-5	2	1	3	1		3

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Cyber Security Fundamentals: Network and Security Concepts-Information Assurance Fundamentals, Basic Cryptography, Symmetric and Asymmetric Encryption, Public Key Encryption, The Domain Name System (DNS), Firewalls, Virtualization, Radio-Frequency Identification.

Threats and vulnerabilities: Types of Threats- Malware, Phishing, Ransomware, Adware and Spyware, Trojan, Virus, Worms, Man-in-the-middle-attack, Scareware, Distributed Denial-Of- Service Attack, Rootkits, click-fraud. Vulnerability-Shellcode, Integer Overflow Vulnerabilities, Buffer Overflows, SQL Injection.

Defense and mitigation measures: Anti-virus scanners, static and dynamic methods, antianalysis, eavading obfuscations and run-time attacks

Cyber Forensics: Memory and network Forensics for Winodws and Linux internals, Forensic tools, OS hardening and RAM dump analysis, data acquisition, data extraction, volatility analyses for OS artifacts and other information. Automated malicous code analysis.

Cybersecurity law and Regulations: Introduction, Cyber Warfare, Deception in the CyberWorld, Legal Framework of Cyber Security.

Learning Resources:

Text Books:

1. James Graham, Richard Howard, Ryan Olson, CYBER SECURITY ESSENTIALS, Taylor and Francis Group, 2011.
2. MarttiLehto, PekkaNeittaanmäki, Cyber Security: Analytics, Technology and Automation, Springer, 2015

Reference Books:

1. David Salomon, Foundations of Computer Security, Springer, 2006

CS26030 **3-0-0 (3)**

Data Hiding

Pre-Requisites: **None**

Course Outcomes:

CO-1	Identify techniques for data hiding.
CO-2	Analyse models of watermarking.
CO-3	Identify different types of attacks.
CO-4	Apply data hiding techniques into different domains.
CO-5	Apply the data hiding techniques in digital rights management.

Course Articulation Matrix:

	PO-1	**PO-2**	**PO-3**	**PO-4**	**PO-5**	**PO-6**
CO-1	1	1		2		2
CO-2	1			2		2
CO-3	1	1		2		1
CO-4		1	2	1		1
CO-5		2	2	2		1

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Introduction: data hiding models, security and privacy aspects, techniques for hiding data Digital audio, video, images and text. Steganography: Introduction, how it is different from cryptography, Classification of steganography algorithms: Transform-based, spatial domain, statistical, other, Applications of steganography: Covert channels, audio data, military, e commerce. Watermarking: Introduction, how it is different from steganography and cryptography, watermarking algorithms, watermarking applications, limitations in watermarking. Digital rights management issues: e-commerce, copyright protection, intellectual property. Issues, digital signatures, authentication, case studies, business models. Multimedia security and information assurance, visual cryptography, key management; Attacks and benchmarks for data hiding systems; Applications of data hiding technology in medicine, law enforcement, remote sensing, and e- commerce, Software for digital data hiding.

Learning Resources:

Text Books:

1. Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, Ton Kalker, *Digital Watermarking and Steganography*, 2nd Edition, Morgan Kaufmann, 2007.
2. Michael T. Raggo and Chet Hosmer, *Data Hiding: Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols*, 1st Edition, Syngress, 2012.

Reference Books:

1. Raggo, Michael T., and Chet Hosmer. "Data hiding." New York. Syngress (2013).

CS26032 DEEP LEARNING 3-0-0: (3)

Pre-Requisites: None

Course Outcomes:

CO1	Identify Convolutional Neural Networks models to solve Supervised Learning Problems.
CO2	Design Autoencoders to solve Unsupervised Learning problems.
CO3	Apply sequence to sequence models for time series analysis classification problems.
CO4	Apply Classical Supervised Tasks for Image Denoising, Segmentation and Object detection problems.

Course Articulation Matrix:

	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	3	2	1	2	1	2
CO-2	2	1	2	2	3	1
CO-3	2	1	2	2	3	3
CO-4	1	2	3	2	3	3
CO-5	3	2	1	2	1	2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Introduction to Biological Neurons, Artificial Neural Networks, McCulloch Pitts Neuron, Learning processes, Perceptron, Perceptron convergence theorem, XOR problem, Multilayer perceptron, Back Propagation Learning, Activation functions, loss functions, Radial Basis Functions. Introduction to Self Organizing Maps; Optimizers: Gradient Descent (GD), Batch Optimization, Momentum Based GD, Stochastic GD, AdaGrad, RMSProp, Adam; Sequence to sequence models, LSTM, BiLSTM, BERT, SciBERT, BioBERT for NLP Applications; Convolutional Neural Network, Building blocks of CNN, Transfer Learning; Regularization: Bias Variance Tradeoff, L2 regularization, Early stopping, Dataset augmentation, Parameter sharing and tying, Dropout; Autoencoders : Unsupervised Learning with Deep Network, Autoencoders, Stacked, Sparse, Denoising Autoencoders, Variational Autoencoders; Recent Trends in Deep Learning Architectures, Residual Network, Skip Connection Network, DensenNet, InceptionNets, SqueezNet, MobileNet, NasNet, HRnet Models; Classical Supervised Tasks with Deep Learning, Segmentation: ResUnet, SegNet, Mask RCNN models, Object Localization: FastRCNN, Faster RCNN, SSD with Applications; Attention Mechanism, Attention Models in Vision; Image Captioning, Visual QA, Visual Dialog, Transformer, Generative Adversarial Network on Image, CycleGANs, Progressive GANs, StackGANs, Unet GAN, vision and NLP Applications.

.Text Books/:

1. Deep Learning- Ian Goodfelllow, Yoshua Benjio, Aaron Courville, The MIT Press.
2. Christopher Bishop, *Pattern Recognition and Machine Learning*, Springer, 2006.

Reference Books

1. Simon Haykin, “Neural Networks, A Comprehensive Foundation”, 2nd Edition, Addison Wesley Longman, 2001.

CS26034 **3-0-0 (3)**

Digital Forensics

Pre-Requisites: **None**

Course Outcomes:

CO-1	Understand the need for digital forensics.
CO-2	Identify different technologies for digital forensics.
CO-3	Understand different investigation methodologies.
CO-4	Apply the digital forensics for different fields.

Course Articulation Matrix:

	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1				1	1	1
CO-2	1			2	1	1
CO-3				2	2	1
CO-4	2		1	2	1	2

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Information formats, PC hardware, Disc geometry, File system, Electronic organizers. Forensic analysis – Investigative Methodology: Forensic Analysis, Electronic Discovery, Intrusion Investigation. Technology: Windows Forensic Analysis, UNIX Forensic Analysis, Embedded Systems Analysis, Mobile Network Investigations. Intrusion Investigation, Analysis tools, Financial forensics.

Learning Resources:

Text Books:

1. Sammes T, B. Jenkinson, *Forensic Computing*, Springer, 2007.

2. Eoghan Casey. Ed., *Handbook of Digital Forensics and Investigation*, Academic Press, 2010.

Reference Books:

1 Grabosky, Peter. Cyber crime and information warfare. Australian Institute of Criminology, 2000.
2 Britz, Marjie. Computer forensics and cyber crime: An introduction, 2/e. Pearson Education India, 2009.

CS26036 **3-0-0 (3)**

Foundations of Blockchain Technology

Pre-Requisites: None

Course Outcomes:

CO-1	To understand the essential concepts and structural components of blockchain and the rationale behind its implementation.
CO-2	To understand the core technology, many types of blockchains and protocols that operate the blockchain.
CO-3	To articulate and develop and test blockchain-compatible diverse applications with smart contracts.
CO-4	To understand and analyze the advantages and disadvantages of employing blockchain technology in various industries and technologies.

Course Articulation Matrix:

	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	2		2	2	-	-
CO-2	2		2	2	2	2
CO-3	3		3	3	3	3
CO-4	3		2	2	2	-

1 - Slightly; 2 - Moderately; 3 - Substantially

Syllabus:

Introduction to Blockchain- Key Concepts of Blockchain, Features of Blockchain, Importance of Blockchain, Blockchain 1.0, 2.0, and 3.0, Issues to Centralized System, Centralized to Decentralized and Distributed System, Building Blocks of Blockchain- Distributed Ledgers & P2P Networks, Block Header, Transaction Organization.

Cryptographic Primitives, Basic Crypto Primitives- Hash Functions- Properties of Hash Function, Nonce, Merkle Trees, Hash Pointers, Public Key Cryptography- Public/private keys, Signature schemes, Signature correctness, Aggregate Signature, Threshold Signature

Decentralization- Distributed shared ledger, Distributed Consensus-Distributed Consensus Protocol. The classical theory of consensus, Byzantine General's Problem possibility and impossibility results, Asynchronous consensus, and Byzantine Fault Tolerance

Types of Blockchain- Permission-less Blockchain- Bitcoin-Introduction to Bitcoin, Bitcoin Transaction, Bitcoin Protocol, Bitcoin Wallets, Bitcoin Block, Bitcoin Scripts, Bitcoin Network, Bitcoin Mining-Nakamoto Consensus- Proof-of-work, Mining target T, Proof-of-work equation, Mining Algorithm, Mining and reward, Block freshness, Partial and full nodes, Attacks on Bitcoin- Double-spend attacks, Selfish mining, **Ethereum Blockchain,** Introduction to Ethereum, Ethereum Networks, Ethereum Wallets, Ethereum Clients, Ethereum accounts, Transactions and State, Smart contracts, Privacy-preserving smart contracts, Proof-of-stake, Variants of Ethereum blockchain

Permissioned Blockchain- Hyperledger Fabric-, State Machine Replication, Distributed State Machines, MSP, Consensus- Raft Consensus Algorithm, Safety and liveness, Privacy based blockchain, ZCash, Zero-knowledge-proof, R3 Corda, Corda Network

Blockchain Security- Attacks on Blockchain and their Countermeasures

Blockchain (BoT) Advantages of integrating Blockchain to IoT, Trust Building, Cost Reduction, Accelerate Data Exchanges, Scaled Security for IoT, IoT Security using BC, Edge Security using BC, Cloud Security using BC, and E2E IoT Security using BC

Learning Resources:

Text Books:

1. Bitcoin and Cryptocurrency Technologies, A. Narayanan, J. Bonneau, E. Felten, A. Miller and S. Goldfeder, Princeton University Press. Henceforth termed as PUP (Princeton university press).
2. Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more, 3rd Edition, Imran Bashir, Packt Publishing, 2020, ISBN: 9781839213199.
3. Introduction to Cryptocurrencies, a basic online course by Haseeb Qureshi.Reference Books:

Reference Books:

1. William Magnuson, “Blockchain Democracy- Technology, Law and the Rule of the Crowd”, Cambridge University Press, 2020.
2. Pethuru Raj, Kavita Saini, Chellammal Surianarayanan, “Blockchain Technology and Applications”, CRC Press, 2021.
3. Chandramouli Subramanian, “Blockchain Technology”, Universities Press, 2020.
4. Relevant Research Paper and While Papers.

CS26038 3-0-0 (3)

Information Security Risk Management

Pre-Requisites: **None**

Course Outcomes:

CO-1	Understand risk-planning and risk management of computer and information systems.
CO-2	Apply vulnerability assessment for natural disaster.
CO-3	Analyzing the implications of emergency response.
CO-4	Design methods for risk mitigation for infrastructure.

Course Articulation Matrix:

	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	1		1	1	1	1
CO-2	2		1	2		2
CO-3	1			1		1
CO-4	2		2	2	1	2

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Development of concepts required for risk-based planning and risk management of computer and information systems (Risk analysis, risk perception, Communicating risk, risk mitigation); Objectives and methods for vulnerability assessment for natural disaster, technological hazards, and terrorist threats; implications for emergency response, vulnerability of critical infrastructures;

Learning Resources:

Text Books:

1. Alan Calder, Steve G. Watkins, Information Security Risk Management for ISO27001/ISO27002, IT Governance, 2010.
2. Susan Snedaker, Chris Rima, Business Continuity and Disaster Recovery Planning for IT Professionals, Elsevier ScienceDirect, second edition, 2014

Reference Books:

1. Harold F. Tipton, Micki Krause Nozaki, Information Security Management Handbook, Volume 6, Sixth Edition, Auerbach Publications, 2016

CS26040 3-0-0 (3)

IoT Security

Pre-Requisites: **CS26002**

Course Outcomes:

CO-1	Ability to Define and implement a security policy.
CO-2	Apply the knowledge to design and build the next generation of smart devices and networked systems.
CO-3	Identify various security issues to detect real-time and capture sensitive data.
CO-4	Understanding of the range of wireless and application protocols that support different IoT application domains.
CO-5	Design or build the reliable, secure system for IoT networks.

Course Articulation Matrix:

	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	–	1	–	–	2	–
CO-2	1	–	–	–	–	–
CO-3	–	–	–	1	–	–
CO-4	–	–	–	–	–	1
CO-5	–	–	1	–	–	–

1 - Slightly; 2 - Moderately; 3 - Substantially

Syllabus:

Introduction to IoT, IoT protocols, Security Requirements, IoT applications and their security/various vulnerabilities, Sensor-based attacks, IoT device-based attacks, Network attacks, attacks against IoT systems (hardware + software) Security issues in SCADA systems, ZIGBEE & BLE, Power analysis attacks, Invasive attacks, Perturbation -attacks, Electromagnetic side-channel attacks, fault injection attack, timing attack, covert channel attacks. M2M Security, RFID Security, Active vulnerability analysis tools, Port scanning, Operating system fingerprinting and version scanning, Penetration testing, Attack surface mapping, Hardware Security, PUF

Privacy Issues of IoT, Trust management in IoT, IoT device authentication, Lightweight authentication techniques in IoT, Blockchain For IoT, Challenges of IoT Addressing Security, Ethics, Privacy, and Laws, Machine Learning-Enabled IoT Security

Learning Resources:

Text Books:

1. Shancang Li, Li Da Xu, Securing the Internet of Things", Syngress, Elsevier, 2017.

2. Fei HU, “Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations”, CRC Press,2016.

Reference Books:

1. Fei Hu, Security and Privacy in Internet of Things (IoTs) Models, Algorithms, and Implementations”, CRC Press, 2016.

CS26042 3-0-0 (3)

Privacy and Security for online social networks

Pre-Requisites: **None**

Course Outcomes:

CO-1	Identify pitfalls in social networks.
CO-2	Analyze trust management in Online social networks.
CO-3	Analyze and apply countermeasures to control information sharing in Online social networks.
CO-4	Apply identity management in Online social networks.
CO-5	APIs to analyze the online social networks.

Course Articulation Matrix:

	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	1		1	2	2	2
CO-2	2		2	2	1	1
CO-3	2		2	2	3	1
CO-4	2		2	3	2	3
CO-5	3		2	2	3	1

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Introduction to Online Social Networks: Introduction to Social Networks, From offline to Online Communities, Online Social Networks, Evolution of Online Social Networks, Analysis and Properties, Security Issues in Online Social Networks, Trust Management in Online Social Networks, Controlled Information Sharing in Online Social Networks, Identity Management in Online Social Networks, data collection from social networks, challenges, opportunities, and pitfalls in online social networks, APIs; Collecting data from Online Social Media

Trust Management in Online Social Networks: Trust and Policies, Trust and Reputation Systems, Trust in Online Social, Trust Properties, Trust Components, Social Trust and Social Capital, Trust Evaluation Models, Trust, credibility, and reputations in social systems; Online social Media and Policing, Information privacy disclosure, revelation and its effects in OSM and online social networks; Phishing in OSM & Identifying fraudulent entities in online social networks

Controlled Information Sharing in Online Social Networks: Access Control Models, Access Control in Online Social Networks, Relationship-Based Access Control, Privacy Settings in Commercial Online Social Networks, Existing Access Control Approaches

Identity Management in Online Social Networks: Identity Management, Digital Identity, Identity Management Models: From Identity 1.0 to Identity 2.0 , Identity Management in Online Social Networks, Identity as Self-Presentation, Identity theft... Open Security Issues in Online Social Networks.

Learning Resources:

Text Books:

1. Security and Privacy-Preserving in Social Networks, Editors: Chbeir, Richard, Al Bouna, Bechara (Eds.), Spinger, 2013.

2. Security and Trust in Online Social Networks, Barbara Carminati, Elena Ferrari, Marco Viviani, Morgan & Claypool publications.

Reference Books:

1. Security and Privacy in Social Networks, Editors: Altshuler, Y., Elovici, Y., Cremers, A.B., Aharony, N., Pentland, A. (Eds.), Springer, 2013

CS26044 **3-0-0 (3)**

Privacy Enhancing Technologies

Pre-Requisites: **None**

Course Outcomes:

CO-1	Analyze the privacy features of social networks.
CO-2	Understand the mechanisms established in trust management.
CO-3	Analyze the Access control models for social networks.
CO-4	Analyze the security issues related to identity management.
CO-5	Analyze the privacy issues in Data Collection.

Course Articulation Matrix:

	PO-1	**PO-2**	**PO-3**	**PO-4**	**PO-5**	**PO-6**
CO-1				1		1
CO-2	2		2	3	1	2
CO-3	2	2	2	3	1	2
CO-4	2		2	3	1	2

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Major issues in computer security related to protecting privacy, threats to the privacy of computer users; Private communications, anonymous communications, censorship circumvention and traffic analysis; Private authentication, selective disclosure credentials for identify management, and zero-knowledge proof techniques; Private statistics and computations through homomorphic encryption and secure multi-party computation and differential privacy; Privacy threats such as pervasive surveillance, profiling, location analysis, and traffic analysis, as well as the technical mitigation techniques relying on modern cryptography and differential privacy; Standard threats to on-line privacy such as profiling, and location analysis; Methods to mitigate abuses arising from anonymous communication, while preserving privacy, through the use of private authentication, and selective disclosure credentials that can be used to build digital cash systems; Zero-knowledge proofs and their use as building blocks of privacy enhancing technologies; Problem of computing on private data using simple homomorphic encryption schemes as well as modern secure multi-party computation techniques; Statistical disclosure control, ad-hoc techniques for analysis and techniques based on differential privacy.

Learning Resources:

Text Books:

1. Benjamin C.M. Fung, Ke Wang, Ada Wai-Chee Fu and Philip S. Yu, Introduction to Privacy-Preserving Data Publishing: Concepts and Techniques, 1st Edition, Chapman & Hall/CRC, 2010.

Reference Books:

1. C C. Aggarwal, Privacy-Preserving Data Mining: Models and Algorithms, 1st Edition, Springer, 2008.
2. Note: Selected research papers are also be given time to time.

CS26046 **3-0-0 (3)**

Public Key Infrastructure and Trust Management

Pre-Requisites: **None**

Course Outcomes:

CO-1	Analyze Core PKI services: Authentication, Integrity, and confidentiality.
CO-2	Design Certificates using Trust Models , PKI Considerations and Electronic Legislation.
CO-3	Identify PKIX standardization Requirements.
CO-4	Distinguish Public key certificate management models.
CO-5	Apply Cryptographic Applications.

Course Articulation Matrix:

	PO-1	**PO-2**	**PO-3**	**PO-4**	**PO-5**	**PO-6**
CO-1	1	1	1	1	1	1
CO-2	2		2	2	2	2
CO-3	1		1	1		1
CO-4	1	1	1	1	1	1
CO-5		1	1	2	1	2

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Introduction – services offered by PKI- components of a fully functional PKI : Certification authority, Certificate repository, Certificate revocation, Key backup and recovery, Automatic key update, Key history management, Cross-certification, Support for non-repudiation, Time stamping, Client software

PKI architectures – Single CA, Hierarchial PKI, Mesh PKI, Trust Lists, Bridge CAs

PKI standards : X.509: Components of X.509: Tamper evident envelope, Basic certificate contents, certificate extensions.; PGP: Web of Trust; Simple PKI (SPKI) / Simple Distributed Security Infrastructure (SDSI): Representing certificates in terms of S-Expressions- Certificate Chain Discovery - Distinct Advantages of SPKI/SDSI over X.509. PKI application : Smart card integration with PKI's

Access Control Mechanisms: Discretionary Access Control (DAC) – Mandatory Access Control (MAC) – Role Based Access Control (RBAC).Issues : Revocation- Anonymity-Privacy issues

Trust Management: Policy based Trust Management System- Social network based Trust Management System- Reputation based Trust Management System (DMRep, EigenRep, P2Prep)- Framework for Trust Establishment. Risks Impact on E-Commerce and E Business: Information Risk – Technology Business Risk.

Learning Resources:

Text Books:

1. Desmedt, Yvo G. (Ed.), *Secure Public Key Infrastructure Standards, PGP and Beyond*, Springer, 2012.

2. J. Camenisch and C. Lambrinoudakis, *Public Key Infrastructures, Services and Applications*, EuroPKI 2010.

Reference Books:

1. Buchmann, Johannes, et al. Introduction to public key infrastructures. Vol. 36. Berlin: Springer, 2013.

CS26048 **3-0-0 (3)**

Scripting languages for information security

Pre-Requisites: **None**

Course Outcomes:

CO-1	Understand, analyze and build dynamic, interactive and secure web sites.
CO-2	Understand current and evolving Web languages for integrating media and user interaction in both front end and back end elements of a Web site.
CO-3	Analysis and reporting of web data and minimizing cyber risks.
CO-4	Applying different testing and debugging techniques and analyzing the web site effectiveness.
CO-5	Applying different cyber security tools and scripting languages to mitigate frequent cyber attacks.

Course Articulation Matrix:

	PO-1	**PO-2**	**PO-3**	**PO-4**	**PO-5**	**PO-6**
CO-1	-	-	2	1	2	1
CO-2	1	1	-	-	2	-
CO-3	2	-	2	1	3	1
CO-4	1	3	-	1	2	3
CO-5	2	1	1	-	3	1

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

HTML: Introduction to HTML, What is HTML, HTML Documents, Basic structure of an HTML document, Creating an HTML document, Mark up Tags, Heading-Paragraphs, Line Breaks, HTML Tags. Elements of HTML: Introduction to elements of HTML, Working with Text, Working with Lists, Tables and Frames, Working with Hyperlinks, Images and Multimedia, Working with Forms and controls.

Java Script: Introduction to JavaScript, Basic Syntax, Control Structures, Writing Functions, Working with Arrays, The Document Object Model, Events Handling, Client-side Validation, Form Validation & RegExps, ASP, Perl CGI, & Form Methods, SSI & Cookies, Frames & Windows, mimeTypes, plugins, & Java

PHP: PHP installation and Introduction, Loops String Functions in PHP, PHP Email Function, PHP Basics, Variables Arrays in PHP with Attributes Date & Time, Image, Uploading File handling in PHP Functions in PHP, Errors handling in PHP.

Python: Introduction to Python, Python basics, Data Types and variables Operators, Looping & Control Structure List, Modules Dictionaries, String Regular Expressions, Functions and Functional Programming, Object Oriented Linux Scripting Environment – Classes, Objects and OOPS concepts, File and Directory Access, Permissions and Controls Socket, Libraries and Functionality Programming, Servers and Clients Web Servers and Client scripting, Exploit Development techniques, Writing plugins in Python, Exploit analysis, Automation Process, Debugging basics, Task Automation with Python

Perl & NodeJS: Introduction to Perl – Overview of Perl Features, Getting and Installing Perl, Accessing Documentation via perldoc, HTML-Format Reference Documentation, Perl Strengths and Limitations, Security Issues in Perl Scripts. Introduction to Node.js; Events; Streams; Modules; Express; Socket.io; Persisting Data

Learning Resources:

Text Books:

1. Deitel, Deitel and Nieto, Internet and Worldwide Web - How to Program, 5th Edition, PHI, 2011.
2. Bai and Ekedhi, The Web Warrior Guide to Web Programming, 3rd Edition, Thomson, 2008.

Reference Books:

1. Computer Programming And Cyber Security for Beginners: Zack Codings (Python Machine Learning, SQL, Linux, Hacking with Kali Linux, Ethical Hacking)

CS26050 **3-0-0 (3)**

Secure Dependable and Distributed Computing

Pre-Requisites: **None**

Course Outcomes:

CO-1	Understand secure development processes in distributed systems.
CO-2	Modeling threats and vulnerabilities for host, network, resident code, storage, grid and applications in distributed computing.
CO-3	Designing architectures for security services in distributed computing.
CO-4	Applying security models for distributed systems.

Course Articulation Matrix:

	PO-1	**PO-2**	**PO-3**	**PO-4**	**PO-5**	**PO-6**
CO-1				1	2	1
CO-2	2		2	2	2	2
CO-3	1		1	2	2	2
CO-4	1		1	2	2	2

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Distributed Systems Security, Secure Development Lifecycle Processes - A Typical Security Engineering Process - Security; Engineering Guidelines and Resources. Common Security Issues and Technologies: Security, Issues, Common Security Techniques; Host-level Threats and Vulnerabilities: Transient code Vulnerabilities - Resident Code; Vulnerabilities - Malware: Trojan Horse – Spyware - Worms/Viruses – Eavesdropping - Job; Faults. Infrastructure-Level Threats and Vulnerabilities: Network-Level Threats and Vulnerabilities - Grid Computing Threats and Vulnerabilities – Storage Threats and Vulnerabilities – Overview of Infrastructure Threats and Vulnerabilities; Application-Level Threats and Vulnerabilities: Application-Layer Vulnerabilities -Injection, Vulnerabilities - Cross-Site Scripting (XSS) - Improper Session Management - Improper Error Handling - Improper Use of Cryptography - Insecure Configuration Issues - Denial of Service - Canonical Representation Flaws - Overflow Issues; Service-Level Threats and Vulnerabilities: SOA and Role of Standards - Service-Level Security Requirements - Service-Level Threats and Vulnerabilities - Service-

Level Attacks - Services Threat Profile; Host-Level Solutions: Sandboxing – Virtualization - Resource Management - Proof-Carrying Code -Memory Firewall – Antimalware. Infrastructure-Level Solutions: Network-Level Solutions - Grid-Level Solutions - Storage Level Solutions; Application-Level Solutions: Application-Level Security Solutions; Service Level Solutions: Services Security Policy - SOA Security Standards Stack – Standards, Deployment Architectures for SOA Security - Managing Service-Level Threats; Future Directions - Cloud Computing Security – Security Appliances, Dependability concepts - Faults and Failures – Redundancy – Reliability – Availability – Safety – Security – Timeliness - Fault-classification - Fault-detection and location - Fault containment, Byzantine failures - Fault injection - Fault-tolerant techniques - Performability metrics, Fault-tolerance in real-time systems - Space- time tradeoff - Fault-tolerant techniques (N-version programming - Recovery block - Imprecise computation; (m,k)-

deadline model) - Adaptive fault-tolerance - Fault detection and location in real-time systems. Security Engineering – Protocols - Hardware protection - Cryptography – Introduction – The Random Oracle model –Symmetric Crypto- primitives – modes of operations – Hash functions – Asymmetric crypto primitives; Distributed systems - Concurrency - fault tolerance and failure recovery – Naming. Multilevel Security – Security policy model – The Bell Lapadula security policy model – Examples of Multilevel secure system – Broader implementation of multilevel security system. Multilateral security – Introduction – Comparison of Chinese wall and the BMA model – Inference Control – The residual problem; Nuclear Command and control – Introduction – The kennedy memorandum – unconditionally secure authentication codes – shared control security – tamper resistance and PAL – Treaty verification. Security printing and seals – Introduction – History – Security printing – packaging and seals – systemic vulnerability – evaluation methodology.

Learning Resources:

Text Books:

1. Ross J Anderson, Ross Anderson, *Security Engineering: A guide to building dependable distributed systems*, Wiley, 2001.
2. David Powell, *A generic fault-Tolerant architecture for Real-Time Dependable Systems*, Springer, 2001.
3. Hassan B Diab and Albert Y. Zomaya, *Dependable computing systems: Paradigm, Performance issues and Applications*, Wiley series on Parallel and Distributed Computing, 2000
4. Abhijit Belapurakar, AnirbanChakrabarti and et al., *Distributed Systems Security: Issues. Processes and Solutions*, Wiley, Ltd., Publication, 2009.

Reference Books:

1. Abhijit Belapurkar, AnirbanChakrabarti, HarigopalPonnapalli, NiranjanVaradarajan, Srinivas Padmanabhuni and Srikanth Sundarrajan, *Distributed Systems Security: Issues, Processes and Solutions*, Wiley publications, 2009.

2. RachidGuerraoui and Franck Petit, *Stabilization, Safety, and Security of Distributed Systems*, Springer, 2010.

CS26052 **3-0-0 (3)**

Secure Operating Systems

Pre-Requisites: **None**

Course Outcomes:

CO-1	Analyze for the vulnerabilities in a given system.
CO-2	Evaluate Information flow secrecy models, integrity models and trust models.
CO-3	Identify the system level security features incorporated in Multics, SELinux, Solaris etc.
CO-4	Assess the security parameters of secure capability systems and secure virtual machines.

Course Articulation Matrix:

	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	3	1	3	1	3	1
CO-2	1	1	1	1	2	3
CO-3	1	1	1	3	1	1
CO-4	1	1	1	2	3	1

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Introduction: Security Goals, Trust Model, Threat Model; Access Control Fundamentals: Protection System, Reference Monitor, Secure Operating System Definition, Assessment Criteria; Multics: Multics History, Multics Security Fundamentals, Multics Protection System Models, Multics Security, Multics Vulnerability Analysis; Security in Ordinary Operating Systems: UNIX Security, UNIX Protection System, UNIX Authorization, UNIX Security Analysis, UNIX Vulnerabilities, Windows Security, Windows Protection System, Windows Authorization, Windows Security Analysis, Windows Vulnerabilities; Verifiable Security Goals: Information Flow, Information Flow Secrecy Models, Denning's Lattice Model, Bell LaPadula Model, Information Flow Integrity Models, Biba Integrity Model, Low-Water Mark Integrity, Clark-Wilson Integrity, The Challenge of Trusted Processes, Covert Channels, Channel Types, Noninterference; Building a Secure Operating System for Linux: Linux Security Modules, LSM History, LSM Implementation, Security-Enhanced Linux, SELinux Reference Monitor, SELinux Protection State, ELinux Labeling State, SELinux Transition State, SELinux Administration, SELinux Trusted Programs, SELinux Security Evaluation; Secure Capability Systems: Capability System Fundamentals, Capability Security, Challenges in Secure Capability Systems, Building Secure Capability Systems; Secure Virtual Machine Systems: Separation Kernels, VAX VMM Security Kernel, Security in Other Virtual Machine Systems.

Learning Resources:

Text Books:

1. Trent Jaeger, *Operating System Security*, Morgan & Claypool, 2008
2. P.G Neumann (PI), *A Provably Secure Operating System*, Final Report published by Stanford Research Institute, California, US., 1975

Reference Books:

1. Morrie Gasser, *Building A Secure Computer System*, Van Nostrand Reinhold, 1988 4. Michael Palmer, *Operating Systems Security*, Thomaon Course Technology, 2004

CS26054 **3-0-0 (3)**

Secure Protocols for Electronic Commerce

Pre-Requisites: **None**

Course Outcomes:

CO-1	Identify algorithms and architecture for security.
CO-2	Classify security for Business-to-Business electronic commerce.
CO-3	Apply the SET Protocol.
CO-4	Evaluate the Secure Payments systems.

Course Articulation Matrix:

	PO-1	**PO-2**	**PO-3**	**PO-4**	**PO-5**	**PO-6**
CO-1	1	1	1	2	1	1
CO-2		1	1	2	1	2
CO-3			2	3		1
CO-4		1	1	2	1	2

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Overview of Electronic Commerce - Electronic Commerce and Mobile Commerce, Effects of the Internet and Mobile Networks, Network Access, Barcodes, Smart Cards, Parties in Electronic Commerce, Security; Money and Payment Systems - Mechanisms of Classical Money, Payment Instruments, Types of Dematerialized Monies, Purses, Holders, and Wallets; Transactional Properties of Dematerialized Currencies, Overall Comparison of the Means of Payment, Practice of Dematerialized Money, Clearance and Settlement in Payment Systems, Drivers of Innovation in Banking and Payment Systems; Algorithms and Architectures for Security - Security of Open Financial Networks, OSI Model for Cryptographic Security, Security Services at the Link Layer, Security Services at the Network Layer, Security Services at the Application Layer, Message Confidentiality, Data Integrity, Identification of the Participants, Biometric Identification, Authentication of the Participants, Access Control, Denial of Service, Nonrepudiation, Secure Management of Cryptographic Keys, Exchange of Secret Keys: Kerberos; Public Key Kerberos, Exchange of Public Keys, Certificate Management, Authentication, Security Cracks; Business-to-Business Commerce-Drivers for Business-to-Business Electronic Commerce, Four Stages of Systems

Integration, Overview of Business-to-Business Commerce, Short History of Business-to Business Electronic Commerce, Examples of Business-to-Business Electronic Commerce, Evolution of Business-to-Business Electronic Commerce, Implementation of Business-to Business Electronic Commerce, X12 and EDIFACT, EDI Messaging, Security of EDI, Integration of XML and Traditional EDI, New Architectures for Business-to-Business Electronic Commerce, Electronic Business (Using) Extensible Markup Language, Web Services, Relation of EDI with Electronic Funds Transfer; Transport Layer Security and Secure Sockets Layer - Architecture of SSL/TLS, SSL/TLS Security Services, SSL/TLS

Subprotocols, Performance of SSL/TLS, Implementation Pitfalls; Wireless Transport Layer Security - Architecture, From TLS to WTLS, Operational Constraints, WAP and TLS Extensions, WAP Browsers; The SET Protocol -SET Architecture, Security Services of SET, Certification, Purchasing Transaction, Optional Procedures, Efforts to Promote SETs, SET versus TLS/SSL; Payments with Magnetic Stripe Cards - Point-of-Sale Transactions, Communication Standards for Card Transactions, Security of Point-of-Sale Transactions, Internet Transactions, 3D Secure, Migration to EMV; Secure Payments with Integrated Circuit Cards - Description of Integrated Circuit Cards, Integration of Smart Cards with Computer Systems, Standards for Integrated Circuit Cards, Multi application Smart Cards, Security of Smart Cards, Payment Applications of Integrated Circuit Cards, EMV® Card, General Consideration on the Security of Smart Cards; Mobile Payments - Reference Model for Mobile Commerce, Secure Element in Mobile Phones; Barcodes, Bluetooth, Near-Field Communication, Text Messages, Bank- Centric Offers, Mobile Operator–Centric Offers, Third-Party Service Offers, Collaborative Offers, Payments from Mobile Terminals; Micropayments - Characteristics of Micropayment Systems, Standardization Efforts, Electronic Purses, Online Micropayments, Market Response to Micropayment Systems; Case Study of PayPal - Evolution of PayPal, Personal Accounts, Business Accounts; Digital Money -Privacy with Cash and Digital Money, DigiCash (eCash), Anonymity and Untraceability in DigiCash, Evaluation of DigiCash; Bitcoin and Cryptocurrencies - Bitcoin Protocol, Operation, Risk Evaluation; Electronic Commerce in Society - Harmonization of Communication Interfaces, Governance of Electronic Money, Protection of Intellectual Property, Electronic Surveillance and Privacy, Content Filtering and Censorship, Taxation of Electronic Commerce, Trust Promotion, Archives Dematerialization

Learning Resources:

Text Books:

1. Mostafa Hashem Sherif, *Protocols for Secure Electronic Commerce*, Third Edition, CRC Press, Taylor and Francis group, 2016
2. Ghosh, Anup K. (Ed.), *E-Commerce Security and Privacy*, Springer Publishing, 2001

Reference Books:

1. Rajaraman, V. Essentials of E-commerce Technology. PHI Learning Pvt. Ltd., 2009.
2. Bidgoli, Hossein. Electronic commerce: principles and practice. Academic press, 2002.

CS26056 **3-0-0 (3)**

Security of E-Based Systems

Pre-Requisites: **None**

Course Outcomes:

CO-1	Propose protocols for e-based systems.
CO-2	Test the protocols using tools.
CO-3	Analyze the e-based systems and identify the issues.
CO-4	Understand fundamentals of authentication protocols.

Course Articulation Matrix:

	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	2		1	2	1	2
CO-2				2		2
CO-3	1		1	2		2
CO-4	1			1		1

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Introduction to Mobile Networks, Wireless Communication Fundamentals, Multi-hop Communication, Impact of mobility.

Cellular networks: Introduction, Frequency Reuse, Channel Assignment Straggles, Handoff Strategy, Inference and system capacity, Improving coverage and capacity.

Medium Access Control: MACA, MACAW, Wireless LAN.

Wireless Sensor Networks (WSN) MAC Protocols: Issues in designing MAC protocols for adhoc wireless networks, design goals, classification of MAC protocols, MAC protocols for sensor network, location discovery, S-MAC, IEEE 802.15.4.

Routing in Mobile Ad hoc Networks (MANET): Ad-hoc On-Demand Distance Vector Routing Protocol (AODV), Dynamic Source Routing (DSR), Secure routing protocols in MANET.

WSN Routing Protocols: Issues in designing a routing protocol, classification of routing protocols, table-driven, on-demand, hybrid, flooding, hierarchical, and power aware routing protocols, WSN Localization methods, Sensor Deployment Strategies, QoS and Energy Management, Underwater sensor networks communication .

5G Architecture: Software Defined Networking – Network Function Virtualization – Basics about RAN Architecture –High-Level Requirements for 5G Architecture – Functional Architecture and 5G Flexibility

Learning Resources:

Text Books:

1. Jochen Schiller, "Mobile Communications", Pearson Education, 2nd Edition, 2003.
2. Ian F.Akyildiz and Mehmet Can Vuran, "Wireless sensor networks ", Wiley Publication.
3. Jonathan Rodriquez, “Fundamentals of 5G Mobile Networks”, Wiley, 2015

Reference Books:

1. Feng Zhao and Leonides Guibas, "Wireless sensor networks ", Elsevier publication - 2004.
2. C. Siva Ram Murthy, and B. S. Manoj, "AdHoc Wireless networks ", Pearson Education - 2008.
3. Asif Oseiran, Jose F.Monserrat and Patrick Marsch, “5G Mobile and Wireless Communications Technology”, Cambridge University Press, 2016.

CS26058 **3-0-0 (3)**

Wireless and Mobile Networks

Pre-Requisites: **None**

Course Outcomes:

CO-1	Identify issues related to environment, communication, protocols in wireless and mobile networks.
CO-2	Understand the functionalities of cellular networks and analyze the methods to improve capacity and coverage.
CO-3	Analyze the performance of MAC protocols for wireless and mobile networks.
CO-4	Evaluate the performance of different routing protocols.
CO-5	Analyze QoS and energy efficiency issues in resource constrained wireless and mobile environment.

Course Articulation Matrix:

	PO-1	**PO-2**	**PO-3**	**PO-4**	**PO-5**	**PO-6**
CO-1	2		2	2	2	
CO-2	2		3	2	2	
CO-3	2		3	2		
CO-4	2		3	2	2	
CO-5	2		2	2	2	

1 - Slightly; **2 - Moderately;** **3 - Substantially**

Syllabus:

Introduction to Mobile Networks, Wireless Communication Fundamentals, Multi-hop Communication, Impact of mobility.

Cellular networks: Introduction, Frequency Reuse, Channel Assignment Straggles, Handoff Strategy, Inference and system capacity, Improving coverage and capacity.

Medium Access Control: MACA, MACAW, Wireless LAN.

Wireless Sensor Networks (WSN) MAC Protocols: Issues in designing MAC protocols for adhoc wireless networks, design goals, classification of MAC protocols, MAC protocols for sensor network, location discovery, S-MAC, IEEE 802.15.4.

Routing in Mobile Ad hoc Networks (MANET): Ad-hoc On-Demand Distance Vector Routing Protocol (AODV), Dynamic Source Routing (DSR), Secure routing protocols in MANET.

WSN Routing Protocols: Issues in designing a routing protocol, classification of routing protocols, table-driven, on-demand, hybrid, flooding, hierarchical, and power aware routing protocols, WSN Localization methods, Sensor Deployment Strategies, QoS and Energy Management, Underwater sensor networks communication .

5G Architecture: Software Defined Networking – Network Function Virtualization – Basics about RAN Architecture –High-Level Requirements for 5G Architecture – Functional Architecture and 5G Flexibility

Learning Resources:

Text Books:

1. Jochen Schiller, "Mobile Communications", Pearson Education, 2nd Edition, 2003.
2. Ian F.Akyildiz and Mehmet Can Vuran, "Wireless sensor networks ", Wiley Publication.

Reference Books:

1. Jonathan Rodriquez, “Fundamentals of 5G Mobile Networks”, Wiley, 2015
2. Feng Zhao and Leonides Guibas, "Wireless sensor networks ", Elsevier publication - 2004.
3. C. Siva Ram Murthy, and B. S. Manoj, "AdHoc Wireless networks ", Pearson Education - 2008.
4. Asif Oseiran, Jose F.Monserrat and Patrick Marsch, “5G Mobile and Wireless Communications Technology”, Cambridge University Press, 2016.