M.TECH. CYBER SECURITY SYSTEMS AND NETWORKS

Amrita Center for Cyber Security Systems and Networks

This M. Tech programme aims to train the students in the cyber security discipline, through a well designed combination of course-ware and its application on real-world scenarios. The programme has a strong emphasis on foundational courses such as mathematics for security applications, advanced algorithms, networks etc., in addition to diverse subject core areas such as cryptography, operating systems & security, cloud security, security of cyber-physical systems etc.

Students will be exposed to real-world problems, open-ended problems, and simulated real-life scenarios with active guidance from domain experts in this field. The program will help the students to:

1. Comprehend the various security threats and vulnerabilities of the cyber world keeping in line with the industrial trends.
2. Scale up to the demand from multiple industrial sectors on the cyber world to promote effective methods, practices and tools to counter the cyber crimes.
3. To be able to architect, design and implement fool-proof product lines in the field of cyber security.

Ultimately this programme will yield next generation cyber security leaders who can be successfully employed in various sectors of industries, business firms, Government departments, financial bodies, educational institutions, etc, and these sectors generate huge demand for well-trained, professional people to be employed on cyber security front and they are always on the look-out for professionally trained people in the area of cyber security.

CURRICULUM

First Semester

Course Code	Type	Course	LTP	Cr
MA619	FC	Advanced Discrete Mathematics	4 0 0	4
SN620	SC	Operating System and Security	3 0 1	4
SN629	FC	Algorithmic Fundamentals for Security	3 0 1	4
SN624	FC	Advanced Computer Networks and Internet Architectures	3 0 1	4
SN627	SC	Principles of Cryptography	3 0 0	3
WN605	SC	Advanced Computer Programming	0 0 1	1
HU601	HU	Cultural Education*		P/F
			Credits:	**20**

*Non-credit course

Second Semester

Course Code	Type	Course	LTP	Cr
MA609	FC	Linear Algebra and Random Process	4 0 0	4
CS622	FC	Parallel and Distributed Systems	3 0 1	4
SN623	SC	Advanced Security of Networked Systems	3 0 1	4
	E	Elective–I	3 0 0	3
	E	Elective–II	3 0 0	3
EN600	HU	Technical Writing*		P/F
			Credits:	**18**

*Non-credit course

Third Semester

Course Code	Type	Course	LTP	Cr
SN621	SC	Database and Application Security	2 0 1	3
	E	Elective –III	3 0 0	3
SN796	P	Live-in-Labs		P/F
SN797	P	Practical Capture the Flag Exercises		P/F
SN799	P	Dissertation		10
			Credits:	**16**

Fourth Semester

Course Code	Type	Course	LTP	Cr
SN799	P	Dissertation		12
			Credits:	**12**

Total Credits: 66

List of Courses

Foundation Core

Course Code	Course	LTP	Cr
MA619	Advanced Discrete Mathematics	4 0 0	4
MA609	Linear Algebra and Random Process	4 0 0	4
SN629	Algorithmic Fundamentals for Security	3 0 1	4
SN624	Advanced Computer Networks and Internet Architectures	3 0 1	4
CS622	Parallel and Distributed Systems	3 0 1	4

Subject Core

Course Code	Course	LTP	Cr
SN620	Operating System and Security	3 0 1	4
SN621	Database and Application Security	2 0 1	3
SN623	Advanced Security of Networked Systems	3 0 1	4
WN605	Advanced Computer Programming	0 0 1	1
SN627	Principles of Cryptography	3 0 0	3

Electives

Course Code	Course	LTP	Cr
	Elective-I		
SN701	Security in the Cloud	3 0 0	3
SN702	Formal Methods	3 0 0	3
SN717	Fundamentals of Data Science and Applications	2 0 1	3
	Elective-II		
SN705	Security of Cyber Physical Systems	3 0 0	3
SN706	Wireless Security	3 0 0	3
SN710	Principles of Machine Learning	3 0 0	3
SN716	Mobile Computing Security	3 0 0	3
	Elective-III		
SN709	Cyber Crimes, Cyber Laws and Cyber Forensics	3 0 0	3
SN713	Software Protection	3 0 0	3
SN 718	Advanced Data Science for Security Analysis	2 0 1	3

Project Work

Course Code	Course	LTP	Cr
SN796	Live-in-Labs		P/F
SN797	Practical Capture the Flag Exercises		P/F
SN799	Dissertation		10
SN799	Dissertation		12

DETAILED SYLLABUS

MA619 ADVANCED DISCRETE MATHEMATICS 4-0-0- 4

Logic, Mathematical reasoning, Sets, Basics of counting, Relations
Graph Theory: Euler graphs,Hamiltonian Paths and circuits,Planargraphs,Trees,Shortest path algorithms, Rooted and binary trees,Distance and centres in a tree,Fundamental circuits and cut sets,Connectivity and separability,Network flows, dominating sets, domination number, Graph colorings and applications,chromaticnumber,Chromatic partitioning, Chromatic polynomial,Matching,vector spaces of a graph.
Analytic Number Theory: Euclid's lemma,Euclidean algorithm,Basic properties of congruences,Residue classes and complete residue systems,Reduced residue systems and the Euler –Fermat theorem,simulataneous linear congruences,Lagrange's theorem and its applications,Wilson's theorem, Chinese remainder theorem,applications of the chinese remainder theorem,primitive roots and reduced residue systems.
Algebra: Groups, subgroups, cyclic groups, abelian groups, permutation groups,grouphomomorphism, normal subgroups,rings, ideal ,ring homomorphism ,Fields,Finite fields and their applications to cryptography.

TEXTBOOKS/REFERENCES:

1. E. Lehman, F.T.Leighton, and Albert R. Meyer, *Mathematics for Computer Science*, MIT OPEN Courseware, 2010.
2. R.P. Grimaldi, *Discrete and Combinatorial Mathematics*, Fifth Edition, Pearson Education, 2007.
3. I.N. Herstein, *Topics in Algebra*, John Wiley and Sons, 2006.
4. K. H. Rosen, *Discrete Mathematics and its Applications*, Seventh Edition, Tata McGraw-Hill Publishing Company Limited, New Delhi, 2007.
5. N. Deo, *Graph Theory with Applications to Engineering and Computer Science*, Prentice Hall of India, New Delhi, 1974.
6. T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, 1976.

SN620 OPERATING SYSTEM AND SECURITY 3-0-1- 4

OS Processes, Synchronization, Memory Management, File Systems
Trusted Operating Systems, Assurance in Trusted Operating Systems, Virtualization Techniques.
Secure operating systems, Security goals, Trust model, Threat model
Access Control Fundamentals – Protection system – Lampson's Access Matrix, Mandatory protection systems, Reference monitor.
Multics – Multics system, Multics security, Multics vulnerability analysis
Security in Ordinary OS – Unix, Windows,
Verifiable security goals – Information flow, Denning's Lattice model, Bell-Lapadula model, Biba integrity model, Covert channels.
Security Kernerls – Secure Communications processor, Securing Commercial OS
Secure Capability Systems – Fundamentals, Security, Challenges
Secure Virtual Machine Systems
Case study - Linux kernel, Android, DVL, Solaris Trusted Extensions

TEXTBOOKS/REFERENCES:

1. Andrew S. Tanenbaum, *Modern Operating Systems*, Third Edition, Prentice Hall, 2007.
2. Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, *Operating System Concepts with Java*", Eighth Edition, Wiley, 2008.
3. Trent Jaeger, *Operating System Security, Synthesis Lectures on Information Security*, *Privacy and Trust*, Morgan and Claypool, 2008.
4. C. P. Pfleeger and S. L. Pfleeger, *Security in Computing*, Prentice Hall Professional, 2003.
5. W. Mauerer, *Professional Linux Kernel Architecture*, Wiley, 2008.
6. D. P. Bovet and M.Cesati, *Understanding the Linux Kernel*, Third Edition, O'Reilly Media, Inc., 2005.

SN629 ALGORITHMIC FUNDAMENTALS FOR SECURITY 3-0-1- 4

Asymptotic Notation and Recurrences: Asymptotic Notation, Recurrences and their solutions, Master's theorem, amortized analysis. Review of combinatorics. Introduction to amortized analysis.
Sorting and searching with corresponding analyses: Bubble sort, Insertion sort, merge sort, quick sort and binary search.
Graph algorithms: BFS, DFS, topological sort, SCC, MST (greedy), SSSP: Dijkstra's and Bellman Ford, APSP (DP). Data structures for disjoint sets.
Greedy technique: Fractional Knapsack, activity selection. Divide-and-Conquer technique: Strassen's algorithm for matrix multiplication, maximum sub-array problem, linear time median. Dynamic programming technique. LC subsequence/substring, 0-1 knapsack, Floyd's APSP, matrix chain multiplication, maximum sub-array problem, rod cutting, party planning, bitonic TSP.
Flow Networks: Ford-Fulkerson method, max flow min-cut theorem, Edmonds Karp algorithm. Maximum bipartite matching.
Number Theory: Preliminaries, Euclid's algorithm and extended Euclid's algorithm.
Introduction to string matching algorithms.
Introduction to NP-Completeness. P, NP, NP-hard, NP-complete, polynomial time reductions.
Approximation algorithms: Vertex cover, TSP with triangle inequality etc..

TEXTBOOKS/REFERENCES:

1. T.H.Cormen, C.E.Leiserson, R.L.Rivest and S.Stein, *Introduction to Algorithms*, Third Edition, MIT Press/McGraw Hill, 2001.
2. Gilles Brassard and Paul Bratley, *Fundamentals of Algorithmics*, PHI, 1996.
3. Rajeev Motwani and Prabhakar Raghavan, *Randomized Algorithms*, Cambridge University Press, 1995.
4. Sanjoy Dasgupta, Christos Papadimitou and U.V.Vazirani, *Algorithms*, McGraw-Hill, 2006.

SN624 ADVANCED COMPUTER NETWORKS AND INTERNET ARCHITECTURES 3-0-1- 4

OSI Layer introduction, Switching topologies
Introduction to Wireless Networks – Wireless LAN technology, Network layer – Internet Addresses, ARP, RARP, IP, Routing algorithm – Interior and Exterior routing. ICMP, Classless and Subnet Address Extensions (CIDR), Internet Multicasting. NAT Routing protocol design and architectures for RIP, OSPF, BGP, RIP- Algorithm of routing, Split horizon, Poison reverse etc., OSPF- OSPF neighbor establishment, database creations,

multiple network types, NBMA, Virtual link scenarios, ABR, ASBR, LSA, Stubby networks etc. BGP-EBGP, IBGP, Mandatory BGP attributes, Next-hop self interactions across ASes, routing loop avoidance, best path selection algorithm TCP and Congestion Control Mechanisms. Quality of service: Quality of Service models, IPP, DiffServ models, dot1p bits, scheduling of traffic. Traffic distribution models and benefits. Internet Architectures- Flow of traffic and routing behavior within Internet, Application of Qos models, application of new resilient designs. Understanding of control and data planes in high end Internet core routers, CEF, hardware packet flows. MPLS, labels, label stacking, packet analysis, RSVP, label allocation, distribution models. MPLS-VPNs- Detailed understanding of MPLS L3 VPNS, routing model employed, forwarding of mplsvpn packets, VRF tables, application scenarios. Implementation in global service provider networks. SocketLevelprogramming,RPC,HighlevelnetworkingusingJava/Python

TEXTBOOKS/REFERENCES:

1. Andrew S. Tanenbaum, *ComputerNetworks*, Fourth Edition, Pearson Education Asia, 2002.
2. Douglas E. Comer, *Internet Working with TCP/IP Volume – I,* Fifth Edition, Prentice Hall, 2008.
3. W. Richard Stevens, Bill Fenner and Andrew M. Rudoff, *Unix Network Programming, Vol.1: The Sockets Networking API*, Third Edition, Addison-Wesley Professional, 2003.
4. Behrouz A. Forouzan and Firouz Musharraf, *Data Communications and Networking*, Fourth Edition, McGraw-Hill, 2007.

SN627 PRINCIPLES OF CRYPTOGRAPHY 3-0-0-3

Probability theory, information theory, complexity theory, numbertheory, abstract algebra (finite fields). Symmetric (Private) Key Cryptographic Systems - Caesar, affine, mono-alphabetic substitutions, transposition, homophonic, Vigenère and Beaufort ciphers, product ciphers, DES and AES. Cryptanalysis of symmetric key ciphers - linear, differential and other cryptanalysis techniques, S-Box design principles, man-in-the-middle attack. Asymmetric (Public) Key Cryptographic Systems (PKCS) - Concepts ofPKCS, RSA cryptosystem, variants of RSA, primality testing, securityof RSA, Wiener's attack on RSA, Merkle-Hellman and ElGamalcryptosystems. Elliptic Curve Cryptography (ECC), attacks on ECC, probabilisticpublic key encryption, pairing based cryptography, the Tate and Weilpairings, identity based encryption, attribute based encryption. Stream Ciphers - The one time pad, synchronous stream ciphers,self-synchronizing stream ciphers, linear feedback shift registers,Berlekamp-Massey algorithm, algebraic attack. Digital Signatures - Rabin, Lamport, Matyas-Meyer, RSA, multiple RSAand ElGamal signatures, digital signature standard, blind signatures,undeniable signatures (Chaum-van Antwerpen), fail-stop signatures (vanHeyst-Pedersen) - Time stamping. Threshold Secret Sharing, Shamir scheme, Blakley scheme and modular scheme.Pseudo Random Number Generators, modern PRNGs. Hash Functions and MACs - Hash functions: the Merkle-Damgardconstruction, Message Authentication Codes (MACs). Boolean functions - discrete Fourier transform on Boolean functions,Parseval's relation, cryptographic criteria for Boolean functions, nonlinearity, balancedness and resiliency, algebraic immunity, bent Boolean functions.

TEXTBOOKS/REFERENCES:

1. Stalling, William, "*Cryptography and Network Security: Principles and Practice*", Fifth Edition, Prentice Hall, 2011.

2. Josef Pieprzyk, Thomas Hardjono and Jenifer Seberry, *Fundamentals of Computer Security*, Springer, 2003.
3. Alfred J Menezes, Paul C Van Oorshot and Scott A.Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
4. Darrel Hankerson, Alfred Menezes and Scott Vanstone, *Guide to Elliptic Curve Cryptography*, Springer 2004.
5. L. Martin, *Introduction to Identity-Based Encryption*, Artech House, 2008.
6. Claude Carlet, *Boolean Functions for Cryptography and Error Correcting Codes,* http://www.math.univ-paris13.fr/~carlet/chap-fcts-Bool-corr.pdf

WN605 ADVANCED COMPUTER PROGRAMMING 0-0-1-1

Programming in C, Basic Computer Organization and Architecture, Build and Compilation process, Debugging concepts, Data Types and Variables, Input/ Output implementation and usage, Control flow, Modular Programming with functions, Stack Frames and Activation Records, Arrays, Pointers, Strings, Structures, Implementation of Structures, Memory, Stacks, Recursion, Dynamic Memory Allocation, Heap, Program Runtime Analysis, Big-Oh Notation.
Significant labs, e.g., Spell Checker with a real dictionary, complicated data structure such as a Vector/Set, Customer Relationship Management system, custom string Abstract Data Type, Maze, etc.

TEXT BOOKS/REFERENCES:

1. Brian W Kernighan and Dennis M Ritchie, "The C Programming Language", Second Edition, Prentice Hall, 1988.
2. K. N. King, "C Programming: A Modern Approach", Second Edition, W. W. Norton and Company, 2008.

MA609 LINEAR ALGEBRA AND RANDOM PROCESS 4-0-0- 4

LinearAlgebra:ReviewofMatrices:Geometryoflinearequations,Vectorspacesandsubspaces,linearindependence,basisanddimensions,lineartransformations,applications of linear transformations, inner product space, orthogonality, Gram Schmidt orthogonalization process,projectionsandleastsquareapplications.
ProbabilityandStatistics:Introductiontoprobabilityconcepts, random variables, probability distributions (continuous and discrete) Bayesianapproachtodistributions,mean and variance of a
distribution,twodimensionalrandomvariablesandjointprobabilitydistributions,stochasticindependenceofrandomvariables,
Theoryofestimation,Bayesianmethodsofestimation,constructionofteststatistics,criticalregion,pvalue.RandomProcesses:generalconcepts,definitions,systemswithstochasticinputs,powerspectrum,discrete-
timeprocesses,randomwalksandotherapplications,ergodicity,Markovchains,transitionprobabilities,classificationofstates,transientandabsorptionprobabilities.

TEXTBOOKS/REFERENCES:

1. Douglas C. Montgomery and George C Runger, *Applied Statistics and Probability For Engineers*, Third Edition, John Wiley and Sons Inc., 2003.

2. EricLehman, F.ThomsonLeighton, and AlbertR.Meyer, *Mathematics for Computer Science*, MIT OPEN Courseware.
3. H. Anton, *Elementary Linear Algebra*, John Wiley and Sons, 2010.
4. A.Papoulis and U.Pillai, *Probability, Random Variables and Stochastic Processes*, Fourth Edition, McGraw Hill, 2002.
5. Ronald E. Walpole, Raymond H Myres, Sharon. L. Myres and KyingYe, *Probability and Statistics for Engineers and Scientists,* Seventh Edition, Pearson Education, 2002.

CS622 PARALLEL AND DISTRIBUTED SYSTEMS 3-0-1- 4

Introduction: Basics of parallelization and parallelization strategies. Parallel/distributed programming models and interfaces - shared memory vs. message passing vs. remote procedure call (RPC) vs. global address space languages: e.g., pthreads, MPI, MapReduce, OpenMP, HPF, UPC, language-level threads (e.g., Java). Parallel machine architectures - shared and distributed memory machines, multicore and multithreaded chips, interconnection networks. Parallel program optimization techniques - synchronization granularity, dependences, scheduling, load balancing. Synchronization - hardware primitives, logical and physical clocks, mutual exclusion, distributed transactions, transactional memory. Consistency and coherence - data-centric versus client-centric consistency models, cache coherence protocols. Fault tolerance and reliability - fail-stop versus byzantine failure models, two- and three-phase commits, reliable group communication, check pointing, message logging.

TEXTBOOKS/ REFERENCES:

1. Anantha Grama, George Karypis, Vipin Kumar and Anshul Gupta, *Introduction to Parallel Computing*, Publishers: Addison-Wesley, 2008.
2. Ajay D. Kshemkalyani and Mukesh Singhal, *Distributed Computing: Principles, Algorithms, and Systems*, Cambridge University Press, 2011.
3. Barry Wilkinson and Michael Allen, *Parallel Programming: Techniques and Applications Using Networked Workstations and Parallel Computers*, Second Edition, Prentice Hall, 2006.
4. George Coulouris, Jean Dollimore, Tim Kindberg and Gordon Blair, *Distributed Systems: Concepts and Design*, Fifth Edition, Addison Wesley, 2012.
5. Salim Hariri and Manish Parashar, *Tools and Environments for Parallel and Distributed Computing*, Wiley-Interscience, 2004.

SN623 ADVANCED SECURITY OF NETWORKED SYSTEMS 3-0-1-4

Network Security Model, Types of Attack, Overview of Most Common Security Issues, Linux Security Overview, Password Attack, Dictionary Attack - Thwarting dictionary attack, IPTables, Using iptables to thwart dictionary attack, Password Cracking - Hashing overview, Lookup tables, Introduction to Rainbow Table, Modern Linux Password Hashing Scheme,
Malware - Virus Infection Techniques, Anatomy of a Virus, Virus Propagation, Classification of Viruses based on Infection Techniques, Memory Strategies etc., Defense Against Viruses, Worms, (Case Study Morris Worm &Conficker worm), Malware analysis, Static and Dynamic Malware analysis,
Application Vulnerabilities – Smashing the Stack for Fun and Profit, Format string attack, SQL Injection, XSS, Authentication- Overview of Authentication, Need for Key Distribution Centers, Authentication & Key Distribution Protocols - Needham Schroeder, Kerberos,

Random Number Generation - Psuedo and True random number generators, Cryptographically Secure PRNGs – The Blum BlumShub Generator, PRNG – Linear Congruential Generators, Entropy - software and hardware, Message Authentication Codes,
TCP/IP Vulnerabilities- TCP Overview - Connection Setup/Teardown, Packet Sniffing, Detecting Sniffers on your network, IP Spoofing, ARP Poisoning, UDP Hijacking, Fragmentation Attack- Ping of Death, Evasion & Denial of Service, UDP Hijacking, TCP Spoofing, TCP Hijacking - Mitnick attack, Joncheray attack, SYN Flood Attack, Denial of Service Attack, Port Scanning Techniques
DNS – DNS Zones, Zone Transfer, BIND, DNS Spoofing, DNS Cache Poisoning, IPSec – Introduction, Tunnel & Transfer Modes, IPSec Authentication Header, Encapsulating Security Header and Payload, IPSec Key Exchange, VPNs S
SL/TLS For Secure Web Services – SSL Connection & SSL Session, SSL Connection State, SSL Session State, SSL Record Protocol, SSL Handshake Protocol, TOR Protocol for Anonymous Routing,
Firewalls – Packet-filtering, Stateless and stateful, Intrusion Detection using SNORT, NAT
Others – Email Spam and solutions, Wireless Security Overview, Cipher Text Attacks

TEXT BOOKS/REFERENCES:

1. Charlie Kaufman, Radia Perlman and Mike Speciner, *Network Security: PRIVATE Communication in a PUBLIC World*, Second Edition, Prentice Hall, 2002.
2. Eric Rescoria, "*SSL and TLS : Designing and Building Secure Systems*, Addison-Wesley Professional, 2000.
3. Stephen Kent, Charles Lynn, Joanne Mikkelson, and Karen Seo, *Secure Border Gateway Protocol (S-BGP)-Real World Performance and Deployment Issues*, NDSS, 2000.
4. Proctor Paul, *The Practical Intrusion Detection Handbook*, Third Edition, Prentice-Hall, Englewood Cliffs, 2001.

EN600 TECHNICAL WRITING P/F

Technical terms- Definitions- extended definitions- grammar checks- error detection- punctuation- spelling and number rules - tone and style- pre-writing techniques - Online and offline library resources- citing references – plagiarism - Graphical representation - documentation styles- instruction manuals- information brochures- research papers, proposals – reports (dissertation, project reports etc.) - Oral presentations.

TEXTBOOKS/REFERENCES:

1. Hirish, Herbert L., *Essential Communication Strategies for Scientists, Engineers and Technology Professionals*, Second Edition, New York: IEEE Press, 2002.
2. Anderson, Paul V., *Technical Communication: A Reader-Centred Approach*, Sixth Edition, Cengage Learning India Pvt. Ltd., New Delhi, Reprint, 2010.
3. Strunk, William Jr. and White, E.B., *The Elements of Style*, Alliyan and Bacon, New York, 1999.

SN621 DATABASE AND APPLICATION SECURITY 2-0-1-3

Database security – Introduction includes threats, vulnerabilities and breaches

Application security – Concepts, CIA Triad, Hexad, types of cyber attacks. Discretionary and Mandatory access control – Principles and applications
Basics of database design: ACID, transaction management and query processing, basic querying tools, data types, integrity constraints and fault tolerance. Database inference problem, distributed database, security levels.
Software development vulnerabilities, code analyzers – Static and dynamic analyzers.
Security in relational data model, concurrency controls and locking.
DB authorization policies, RBAC – concepts and applications, biometric DB authorization, concepts of DB audit. SQL extensions to security with Oracle as an example. MAC Concepts and multi-level secure data base concepts, Polyinstantiation
System R concepts, Context and control based access control, Oracle VPD
Privacy preservation, anonymization and Hippocratic databases: Principles and architecture. Inference – An in-depth treatment, types of inference attacks
Biometric security concepts. XML security, Multi-level object DB security.
Security in data warehouses and OLAP systems. Database watermarking – Concepts and copyright protection. Managing and querying encrypted data
DB issues in trust management and trust negotiation

TEXTBOOKS/ REFERENCES:

1. Michael Gertz and Sushil Jajodia, *Handbook of Database Security—Applications and Trends*, Springer, 2008.
2. Basta, Alfred, and Melissa Zgola, *Database Security*, Cengage Learning, 2011.

SN701 SECURITY IN THE CLOUD 3-0-0- 3

Introduction to cloud computing- Evolution of cloud computing, Definition of cloud computing, SPI framework, Service delivery model, Deployment models, Key drivers to adopting the cloud, Barriers to cloud computing adoption in the cloud, Modular arithmetic background, concepts of security, how to assess security of a system, information theoretic security v/s computational security, Data security and storage in cloud, data dispersal techniques, High-availability and integrity layer for cloud storage, Encryption and key management in the cloud, Cloud forensics, Data location and availability, Data security tools and techniques for the cloud, Data distribution and information dispersal techniques, Data encryption/decryption methodologies and algorithms for a client-server setup such as SSL, IPSec, etc., Introduction to Homomorphic encryption. Approximate string searching over encrypted data stored in the cloud, Trustworthy cloud infrastructures, Secure computations, Cloud related regulatory and compliance issues.

TEXTBOOKS/REFERENCES:

1. Tim Mather, S. Kumaraswamy and S. Latif, *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance,* O'Reilly Media, 2009.
2. William Stallings, "*Cryptography and Network Security: Principles and Practice*, Fifth Edition, Prentice Hall, 2011.
3. Menezes. A, Oorschot. P, and Vanstone. S, *Handbook of Applied Cryptography*, CRC Press, 1996.
4. B. Schneier, "*Applied Cryptography: Protocols, Algorithms, and Source Code in C",* Second Edition, John Wiley and Sons, 1996.
5. Terrence Lillard, "*Digital Forensics for Network, Internet, and Cloud Computing*, Elsevier, 2010.

SN702 FORMAL METHODS 3-0-0- 3

Background: Computability and Complexity
Decidability, Semi-decidability, Undecidability, Halting problem, Rice's theorem
Overview of complexity classes: P, NP, NP-completeness.
Propositional and First-Order Logic: Syntax, Semantics, Proof methods
Program Verification: Floyd-Hoare logic, Weakest Pre-conditions; Partial Correctness and Termination Structural induction and Fixed-point induction for recursive procedures
Z specification language: Fundamentals and abstract datatype specifications.
Data refinement in Z abstract data types: Forward and backward simulation, Concurrent Programs and Correctness Properties: Owick-Gries, Assume-Guarantee
Reactive Systems: Transformational vs Reactive systems, Temporal Logic: Linear (LTL) and Branching Time (CTL), Temporal specification of reactive systems: Safety, Liveness, Fairness, Buchi automata, LTL-to-Buchi automata, Properties: containment, emptiness
Model Checking: LTL and CTL model-checking. Analysis of model-checking algorithms Symbolic model checking; overview of state-space reduction methods, Case study and practical verification of properties
Process Algebra: CCS and Pi-calculus, Reductions and labelled transitions, Harmony lemma, Bisimulations

TEXTBOOKS/REFERENCES:

1. E.M. Clarke, O. Grumberg, and D. Peled, *Model Checking*, MIT Press, 2000.
2. Davide Sangiorgi and David Walker, *Pi-Calculus: The Theory of Mobile Processes*, Cambridge University Press, 2001.
3. Sanjeev Arora and Boaz Barak, *Computational Complexity – A Modern Approach*, Cambridge University Press, 2009.
4. Michael Huth and Mark Ryan, *Logic in Computer Science*, Cambridge University Press, 2004.
5. J. Woodcock and J. Davies, *Using Z: Specification, Refinement and Proof*, Prentice Hall, 1994.

SN705 SECURITY OF CYBER PHYSICAL SYSTEMS 3-0-0- 3

Security and vulnerability of cyber-physical infrastructure networks, game theory for infrastructure security, An analytical framework for cyber-physical networks, Mobile and wireless network security, Robust wireless infrastructure against jamming attacks, Security of Mobile Adhoc networks, Defending against indentity based Attacks in wireless networks, Security of sensor networks , Hardare&Security:Vulnerabilities& Solutions, Languages and Security: Safer software through Language and Compiler techniques, Cloud computing and data security, Event Awareness and System Monitoring for Cyber Physical Infrastructure, Pervasive Sensing and Monitoring for Situational Awareness, Managing and Securing Critical Infrastructure with Semantic Policy and Trust-Driven Approach, Policies, Acess Control and Formal Methods, Formal Analysis of Policy-Based Security Configuarations in Enterprise Networks, Security and Privacy in Smart Grid, Automotive Information Technology, Mobile Health-Care (m-health) systems, VoIP Telecommunication Networks.

TEXTBOOKS/REFERENCES:

1. Sajal Das, Krishna Kant, and Nan Zhang, *Securing Cyber-Physical Critical Infrastructure – Foundations & Challenges*, Morgan Kaufmann, 2012.

SN 706 WIRELESS SECURITY 3-0-0- 3

Wireless Network Operation: Wireless Network Topologies, Cellular Topology, Cell Fundamentals, Signal to Interface Ratio, Mobility Management, Radio Resources and Power Management, Security in Wireless Networks. Wireless WANs: GSM & TDMA, Mobile Environment, Communications in the Infrastructure, CDMA Technology, Reference Architecture for North American Systems, IMT-2000, Data Oriented CDPD Networks, GPRS, SMS, Mobile Application Protocol. Local Area & Ad Hoc Networks: LAN Technologies, Evolution of Wireless LAN, Current Technology and Market Scenario, IEEE 802.11, Physical, Layer, MAC Sublayer, Wireless ATM, HYPERLAN, IEEE 802.15 Wireless PAN, Home RF, Bluetooth IrDA. Clustering Security in Wireless Networks: Issues of security in wireless; IP broadcast, Satellite broadcast; issues of information capacity; issues of 802.11 protocols; design of secure protocols; Secure routing — Secure localization — Secure and resilient data aggregation — Key pre-distribution and management. Encryption and authentication — Security in group communication — Impact on IP stack from MAC layer and up; source authentication of transmissions, and non-repudiation; Power management and selfishness issues, attacks in wireless networks; DOS and DDOS attacks, reaction to attacks, information processing for sensor networks.

TEXT BOOKS/REFERENCES:

1. Nicholos Lekkas, *Wireless Security,* McGraw-Hill, 2000.
2. KavehPahlavan and Prashant Krishnamurthy, *Principles of Wireless Networks*, Prentice Hall, 2006.

SN709 CYBER CRIMES, CYBER LAWS AND CYBER FORENSICS 3-0-0- 3

Introduction to IT laws & Cyber Crimes – India and International perspectives, Governance and Legal Issues.

Principles of Digital investigations, Hardware forensics tools – Single purpose, Computer networks and Servers Software forensics tools, Log file analysis, Cloud forensics, Analysis of Acquisition, Validation, Discrimination, Extraction, Reconstruction, Reporting, Forensics examination protocols, NIST forensics Tools. Crime-specific Digital Triage Process. Operating System and File System Forensics, Detecting Data Concealment Programs Using Passive File System Analysis, Assessing Trace Evidence Left by Secure Deletion Programs.

Architecture for SCADA Network Forensics.- Portable Electronic Device Forensics, Data Forensics - Data Fingerprinting

Theoretical Interpretations and Modeling in Forensics - Applications of Graph theory and Bayesian models.Applying Machine Trust Models to Forensic Investigations.- Exploring Big Haystacks.- Forensic Techniques.- Countering Hostile Forensic Techniques

TEXTBOOKS/REFERENCES:

1. A. Vishwanathan, *Cyber Law – Indian and International Perspectives on Key Topics*, LexisNexis Publishers, ISBN: 9788180387395, 2012.
2. Bill Nelson, Amelia Philips and Christopher Steuart, "*Guide to Computer Forensics and Investigations*", Fourth Edition, Cengage Learning, ISBN: 1-435-49883-6, 2009.
3. Eoghan Casey, *Handbook Computer Crime Investigation's Forensic Tools and Technology*, First Edition, Academic Press, 2001.
4. Olivier, Martin S., and Sujeet Shenoi, (eds), *Advances in Digital Forensics II, Vol. 222*, Springer, 2006.

5. Peterson, Gilbert, and Sujeet Shenoi, *Advances in Digital Forensics IX, Vol. 410*, Springer, 2013.

SN710 PRINCIPLES OF MACHINE LEARNING 3-0-0- 3

Roleoflearninginintelligentbehavior,Designingalearningsystem;learningfromexample;Concept learning,Bayesiandecisiontheory,BayesianLearning,Decisiontreelearning:UnivariateTrees,ClassificationTrees,RegressionTrees,RuleExtractionfromTrees,LearningRulesfromData,lineardiscrimination,SVMs:linearSVMs,introductiontokernelmethods,multilayerperceptrons,Localmodels,CompetitiveLearning,IncorporatingRule-BasedKnowledge,ComputationalLearningTheory,InstancebasedLearning,LearningsetsofRules,AnalyticalLearning,Boostingalgorithms,Combiningmultiplelearners,Reinforcementlearning.

TEXTBOOKS/REFERENCES:

1. Tom Michael, *Machine Learning*, McGraw Hill, 1997.
2. E.Alpaydin, *Introduction to Machine Learning*, PHI, 2005.
3. T. Hastie, R.TIbshirani and J. Friedman, *Machine Learning*, McGraw Hill, 1997.
4. T. Hastie, R.TIbshiran, and J. Friedman, *The Elements of Statistical Learning,* Springer, 2001.
5. Y.N.Vapnik, *The Nature of Statistical Learning Theory*, Springer, 1999.

SN 713 SOFTWARE PROTECTION 3-0-0- 3

Introduction: Software Protection: What, why, how.
Setting up software analysis lab. State-of-the-art tools. Protocol for handling potentially malicious programs. Legal issues.
Offensive and Defensive strategies - Offense – Motivation, Methods of attacking software protection. Defense: Methods for hiding information, purpose, algorithms in software.
Program Analysis Static analysis: Control flow analysis, data flow analysis, dependence analysis.
Dynamic analysis: Debugging, tracing, profiling, emulation.
Static Code obfuscation - In-depth Semantics preserving obfuscating transformations, complicating control flow, opaque predicates, data encoding, breaking abstractions.
Obfuscation – Theoretical Bounds Various impossibility results.
Tamper roofing and Watermarking Definitions, Algorithms for Tamperproofing, Remote Tamperproofing.
Watermarking Definitions, Methods of Watermarking, Tamperproofing watermarks, Resilient watermarks, Stealth watermarks. Steganographic watermarks, Dynamic watermarking.
Software Similarity Analysis:- Alternate methos for defeating obfuscations. K-gram based analysis, API-Based analysis, Tree-based Analysis, Graph-Based analysis, Metrics-Based Analysis.

TEXTBOOKS/ REFERENCES:

1. Christian Collberg and Jasvir Nagra, *Surreptitious Software: Obfuscation, Watermarking, and Tamperproofing for Software Protection*, Addison-Wesley, 2010.

SN 716 MOBILE COMPUTING AND SECURITY 3-0-0- 3

Introduction to Mobile Computing: Mobile Computing Models, Design and Implementation, Mobile Architecture, Service Discovery protocol, Mobile P2P systems,

Mobile Networking; **Security in Mobile Computing:** Information flow tracking, Privacy, Application Security, Execution transparency; **Situation Awareness:** Situation Models, Modeling situation awareness, Modelling Context and User; **Location awareness:** Indoor localization – Radar, Horus, Outdoor localization – Global Positioning Satellite, Assisted Global Positioning Satellite; **Context-Aware Computing:** Context modeling, Ontological based approach, Context Reasoning, Context-aware systems, Middleware in Context Aware Computing, Context-aware security, Proactive Computing.

TEXTBOOKS / REFERENCES:

1. F. Adelstein, S.K.S. Gupta, G.G. Richard III and L. Schwiebert, *Fundamentals of Mobile and Pervasive Computing*, McGraw Hill, ISBN: 0-07-141237-9, 2005.

This will be a research paper based course. Students are expected to read, summarize and discuss assigned research papers in the field for each class.

SN 717 FUNDAMENTALS OF DATA SCIENCE AND APPLICATIONS 2-0-1- 3

Data Stores - Introduction to Structured Data, DBMS Concepts, RDBMS (Oracle/MySQL), NoSQL Concepts, Mongo, Cassandra, Basic to complex Querying in SQL. (Lab Element), Query tuning., Introduction to Unstructured Data, Taming Unstructured Data. Understanding Data - Understanding data formats (XML, JSON, YAML, PMML), Data feeds (RSS, Atom, RDF), Preparing Data - Data Analysis/Profiling, Data Cleansing.
OLTP & OLAP - Fundamentals of Data Warehousing, Dimension Modeling., Slowly Changing Dimensions, ETL Process, Performance Tuning of warehouse Loads, Data Analytics Fundamentals, Pre Processors, Post Processors
Supervised Learning - Linear/Logistic Regression, Decision Tree, Naïve Bayes
Unsupervised Learning, K-Means, Association Rules, Hands on implementation of the basic algorithms.
Introduction to Hadoop, Map-Reduce. Hadoop Theory and hands on implementation, MR coding, Basic Management and Monitoring of Hadoop Cluster, Implementation of K-means algorithm using MR.
Introduction to Streaming Data Analytics, Introduction to Spark, Introduction to Storm, Introduction to Scala.

TEXTBOOKS/REFERENCES:

1. C. O'Neil, and R. Schutt, *Doing Data Science* – Straight Talk from Frontline Tom Michael, *Machine Learning*, McGraw Hill, 1997.
2. T. Hastie, R. Tibshirani and J. Friedman, *Elements of Statistical Learning – Data Mining, Inference, Prediction,* Springer, 2003.

SN 718 ADVANCED DATA SCIENCE FOR SECURITY ANALYSIS 2-0-1- 3

Handling Streaming Data - In-memory Analytics using Spark, Introduction to Redis, Using Redis in Spark for In-mem analytics, Message Brokers (MQTT, Kafka, Active MQ), CMS, HLL algorithms, Social media Analytics, Streaming Sensor Data Analytics, Introduction to Streaming Algorithms
Advanced Hadoop& MR, Implementing complex algorithms using MR, Analytics HDFS data in Spark (in-memory) using Shark and Spark SQL, Implementing Slowly changing dimensions in Hadoop based Data warehouses.

Big Data Warehouse - Hadoop Ecosystem, HBase, Pig & Pig Latin, Sqoop, ZooKeeper, Hue, Hive,Flume,Oozie
Security Concerns in Big data, Visualization techniques in Big Data Analytics, Case Study & Implementation

TEXTBOOKS/REFERENCES:

1. A. Rajaraman and J. D. Ullman, *Mining of Massive Datasets*, Cambridge University Press, 2012.
2. N. Burlingame, *The Little Book of Big Data*, New Street Communications, LLC, Wickford, 2012.