Master of Technology (Cyber Security)

Department of
Computer Science & Engineering

SPUP
SARDAR PATEL UNIVERSITY OF
POLICE, SECURITY AND CRIMINAL JUSTICE
JODHPUR

Sardar Patel University of Police, Security and Criminal Justice, Jodhpur
(Established Under State Legislative Assembly Act of Government of Rajasthan)

About the Department

The Department of Computer Science & Engineering was established in 2013. The department offers 2-years MTech programme in Cyber Security.

About the Programme

Cyber security is an emerging area in the field of Computer Science & Engineering. M.Tech in Cyber Security is aimed at producing the much needed highly skilled manpower in the area of Information Security. It offers many areas for specialization including: securing network(s) and allied infrastructure, securing applications, security testing, information testing, information systems auditing, penetration testing, forensic investigation and digital forensics science etc. Keeping all the facts in view this program is designed to create professionals trained in both cyber forensics and cyber security with best of technical talent.

The objectives of the course are:
.

- To develop a human resource specialized in cybercrime investigation, which can be assistance to our law enforcement agencies.
- To prepare trained manpower in cyber security required in academics, industries and research organizations.
- The approach shall be both multidisciplinary and interdisciplinary.

Scheme and Detailed Syllabus

M.TECH. CYBER SECURITY

[*Revised syllabus to be effective from session 2019 for batch 2019-21 and subsequent batches.*]

Sem	Sub. Code	Title of the subject	Credits	Contact hours / week		
				L	T	P
I	1CS01	Mathematical Foundations of Cyber Security	4	4	-	-
	1CS02	Topics in Cyber Security	4	3	-	2
	1CS03	Cyber Crime, Cyber Laws and IPR	4	4	-	-
	1CS04	Wireless Networks: Security and Privacy	4	3	-	2
	1CSxx	Program Elective - I	4			
	1CSxx	Program Elective - II	4			
II	2CS05	Applied Cryptography	4	3	-	2
	2CS06	Cyber Forensics, Audit and Investigation	4	3	-	2
	2CS07	Web Application and Penetration Testing	4	3	-	2
	2CS08	Malware Analysis & Network Security	4	3	-	2
	2CSxx	Program Elective III	4			
	2CSxx	Program Elective IV	4			
III						
	3CS09	Dissertation I	16			32
IV						
	4CS10	Dissertation II	16			32

List of Electives

Following list has to be used for offering programme elective I and II. Additional Elective can be added as and when required after taking departmental approval.

Sub. Code	Title of the subject	Credits	Contact hours / week		
			L	T	P
Group A (Program Elective I & II)					
1CS51	Cloud Computing	4	3	1	
1CS52	E Commerce	4	4		
1CS53	Neural Networks	4	3		2
1CS54	Data Mining	4	3		2
1CS55	Information Security and Privacy	4	3	1	
1CS56	Security Analysis of Protocols	4	3	1	
Group A (Program Elective III & IV)					
2CS57	Banking Technology and Management	4	4		
2CS58	Big Data Analytics	4	3		2
2CS59	Machine Learning	4	3	1	
2CS60	Cloud Computing and Security	4	3	1	
2CS61	Introduction of evolutionary computing	4	4		
2CS62	Internet of Things and Security	4	3		2

Students can also elect subjects offered by online MOOC portals (NPTEL, SWAYAM, etc.) as Program Elective after departmental approval.

MATHEMATICAL FOUNDATIONS FOR CYBER SECURITY

Course Credits: 4 (4-0-0)   **1CS01**

Unit I
Number Theory: Introduction - Divisibility - Greatest common divisor - Prime numbers - Fundamental theorem of arithmetic - Mersenne primes - Fermat numbers - Euclidean algorithm - Fermat's theorem - Euler totient function - Euler's theoerem. Congruences: Definition - Basic properties of congruences - Residue classes - Chinese remainder theorem.

Unit II
Algebraic Structures: Groups – Cyclic groups, Cosets, Modulo groups - Primitive roots - Discrete logarithms. Rings – Sub rings, ideals and quotient rings, Integral domains. Fields – Finite fields – GF (p^n), $GF(2^n)$ - Classification - Structure of finite fields. Lattice, Lattice as Algebraic system, sub lattices, some special lattices.

Unit III
Probability Theory: Introduction – Concepts of Probability - Conditional Probability - Baye's Theorem - Random Variables – discrete and continuous- central Limit Theorem-Stochastic ProcessMarkov Chain.

Unit IV
Coding Theory: Introduction - Basic concepts: codes, minimum distance, equivalence of codes, Linear codes - Linear codes - Generator matrices and parity-check matrices - Syndrome decoding – Hamming codes - Hadamard Code - Goppa codes.

Unit V
Pseudorandom Number Generation: Introduction and examples - Indistinguishability of Probability Distributions - Next Bit Predictors - The Blum-Blum-Shub Generator – Security of the BBS Generator.

Books recommended:
- D. S. Malik, J. Mordeson, M. K. Sen, Fundamentals of abstract algebra, Tata McGraw Hill

- P. K. Saikia, Linear algebra, Pearson Education, 2009.

- I. Niven, H.S. Zuckerman and H. L. Montgomery, An introduction to the theory of numbers, John Wiley and Sons, 2004.

- D P Bersekas and J N Tsitsiklis, Introduction to probability, Athena Scientific, 2008

- Douglas Stinson, 'Cryptography – Theory and Practice', CRC Press, 2006.

- Sheldon M Ross, "Introduction to Probability Models", Academic Press, 2003.

- C.L. Liu, 'Elements of Discrete mathematics', McGraw Hill, 2008.

- Fraleigh J. B., 'A first course in abstract algebra', Narosa, 1990.

- Joseph A. Gallian, ''Contemporary Abstract Algebra', Narosa, 1998

TOPICS IN CYBER SECURITY

Course Credits: 4 (3-0-2)   **1CS02**

Unit I
Topics in Data Structures: Various Trees, Linked List, Heap, Stack, Queues. Abstract Data Types using Python and C Language.

Unit II
Topics in Data Base Management Systems: Entity–Relationship model (E-R model) – E-R Diagrams, Functional Dependencies – Non-loss Decomposition, First, Second, Third Normal Forms, Dependency Preservation – Boyce/Codd Normal Form- Multi-Valued Dependencies and Fourth Normal Form – Join Dependencies and Fifth Normal Form, Two Phase Commit, ACID Property, Two Phase Locking –Intent Locking – Deadlock- Serializability, Magnetic Disks – RAID – Tertiary storage – File Organization

Unit III
Topics in Algorithms: Algorithm Development, Complexity analysis, Sorting, Searching, BFS, DFS, Minimum Spanning Tree, Prim's and Kruskal';s algorithms, Greedy algorithms – Divide and conquer – Dynamic programming – backtracking– algorithm analysis

Unit IV
Topics in Operating System: Overview of operating systems, functionalities and characteristics of OS, concept of a process, operations on processes, process states, concurrent processes, process control block, process context, Job and processor scheduling, scheduling algorithms, Deadlock: prevention, detection, avoidance, banker';s algorithm, Memory organization and management, storage allocation Android OS, iOS, Linux OS file structure and security features

Unit V
Topics in Computer networks: OSI Model and each layer working, properties and related protocols in security areas.

Books recommended:
- Introduction to Algorithms by Thomas H. Cormen

- The Practice of Programming by Kernighan

- Advanced Programming in the Unix Environment by W. Richard Stevens

- Abraham Silberschatz, Henry F. Korth, S. Sudharshan, "Database System Concepts", Tata McGraw Hill

- Ramez Elmasri, Shamkant B. Navathe, "Fundamentals of Database Systems"

- A. V. Aho, J. E. Hopcroft, and J. D. Ullman, "Data Structures and Algorithms", Pearson Education

- Andrew Tanenbaum, Modern Operating Systems, Prentice Hall.

- James F. Kuross, Keith W. Ross, "Computer Networking, A Top-Down Approach Featuring the Internet", Addison Wesley

- Andrew S. Tanenbaum, "Computer Networks"

CYBER CRIME, CYBER LAWS AND IPR

Course Credits: 4 (4-0-0)   **1CS03**

Unit I
Introduction to cyber crime and cyber law, cyber space and information technology, Nature and scope of cyber crime, Jurisdiction of cyber crime.

Unit II
Important definitions under IT Act 2000, Cyber crime issues: unauthorized access, White collar crimes, viruses, malwares, worms, Trojans, logic bomb, Cyber stalking, voyeurism, obscenity in internet, Software piracy,

Unit III
IT Act 2000, offences under IT Act and IT (amendment) Act, 2008. CRPC overview, Case studies, Role of intermediaries, Electronic evidence, Cyber terrorism, espionage, warfare and protected system

Unit IV
Overview of amended laws by the IT Act, 2000: The Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Banker's Book Evidence Act, 1891, The Reserve Bank of India Act, 1934, Cyber Theft and the Indian Telegraph Act, 1885. Relevant Case laws. Digital Signatures and certificate - legal issues

Unit V
Intellectual Property rights: Introduction to IP, Copyright, Related Rights, Trademarks, Geographical Indications, Industrial Design, Patents, Licensing and transfer of technology, WIPO Treaties, Copyrights Act, Patents Act, Trademarks Act

Books recommended:
- Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives, Raghu Santanam, M. Sethumadhavan, Information Science Reference

- Pfleeger, Charles P. and Shari L. Pfleeger. Security in Computing, 4th Edition. Upper Saddle River, NJ: Prentice Hall, 2008

- Cybercrime: Security and Surveillance in the Information Age, Douglas Thomas; Brian Loader

- Computer Crime: A Crime-Fighters Handbook by David Icove

- Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities, Peter N. Grabosky

- Cyberlaw – The Indian Perspective By Pavan Duggal, Saakshar Law Publications.

- Jonathan Rosenoer,"Cyber Law: The law of the Internet", Springer-Verlag, 1997

- Mark F Grady, FransescoParisi, "The Law and Economics of Cyber Security", Cambridge University Press, 2006

WIRELESS NETWORKS: SECURITY & PRIVACY

Course Credits: 4 (3-0-2)   **1CS04**

Unit I

Wireless Networking Trends, Key Wireless Physical Layer Concepts: Frequency, Wavelength, Phase, Coding and modulation, Shannon Theorem, Hamming Distance, Multiple Access Methods, Doppler Shift; Signal Propagation: Reflection, Diffraction, Scattering, Fading, Shadowing, Multipath, MultiAntenna Systems, Beam forming, MIMO, OFDM; Wireless Local Area Networks: IEEE 802.11, Amendments; Wireless Personal Area Networks,

Unit II

GSM: Overview, Architecture, GSM Security Principles; General Packet Radio Services (GPRS): Overview, Architecture; Universal Mobile Telecommunication System (UMTS): Overview, Architecture and Subsystems; LTE: Overview, Architecture and Subsystems;

Unit III

Radio Frequency Identification (RFID); WiMAX (Physical layer, Media access control, Mobility and Networking); Multi hop wireless networks: Position & topology base ad-hoc routing protocols, Proactive and Reactive routing protocols. Route disruption, diversion, routing state based attacks, SRP, Ariadne, SAODV, ARAN, SMT secure routing protocols, Wireless Sensor Networks,

Unit IV

Security of wireless networks: GSM, UMTS, WEP, IEEE 802.11i, Public Wifi hotspots, Bluetooth; Vehicular Ad-hoc Networks: vulnerabilities, challenges, Security architecture

Unit V

Naming & addressing principles, attacks and protection techniques, Misbehaviour at MAC layer of CSMA/CA, its impact and preventive measures, Mobile IPv4, Mobile IPv6, TCP over Wireless Networks

Books recommended:
- Jochen Schiller, "Mobile Communications", PHI.

- K Makki, P Reiher,et. all. "Mobile and Wireless Network Security and Privacy",Springer, 2007

- LeventeButtyan, J P Hubaux. "Security and Cooperation in Wireless Networks", Cambridge University Press, 2008.

- Uwe Hansmann, LotharMerk, Martin S. Nicklons and Thomas Stober, Principles of Mobile Computing, Springer, New York, 2003

- Frank Adelstein, Sandeep KS Gupta, Golden Richard, Fundamentals of Mobile and Pervasive Computing,McGraw-Hill

- Butty L. &Hubaux J.P. (2007): Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing, Cambridge University Press.

- Wireless Ad hoc and Sensor Networks – Protocols, Performance and Control, JagannathanSarangapani, CRC Press, Taylor & Francis Group, 2007

APPLIED CRYPTOGRAPHY

Course Credits: 4 (3-0-2)   **2CS05**

Unit I
Foundations – Protocol Building Blocks - Basic Protocols - Intermediate Protocols - Advanced Protocols - Zero-Knowledge Proofs - Zero-Knowledge Proofs of Identity -Blind Signatures - Identity-Based Public-Key Cryptography - Oblivious Transfer - Oblivious Signatures - Esoteric Protocols

Unit II
Key Length - Key Management - Electronic Codebook Mode - Block Replay - Cipher Block Chaining Mode - Stream Ciphers - Self-Synchronizing Stream Ciphers - Cipher-Feedback Mode - Synchronous Stream Ciphers - Output-Feedback Mode - Counter Mode - Choosing a Cipher Mode - Interleaving - Block Ciphers versus Stream Ciphers - Choosing an Algorithm - PublicKey Cryptography versus Symmetric Cryptography - Encrypting Communications Channels - Encrypting Data for Storage - Hardware Encryption versus Software Encryption - Compression, Encoding, and Encryption - Detecting Encryption – Hiding and Destroying Information.

Unit III
Information Theory - Complexity Theory - Number Theory - Factoring - Prime Number Generation - Discrete Logarithms in a Finite Field - Data Encryption Standard (DES) – Lucifer -Madryga - NewDES - GOST – 3 Way – Crab – RC5 - Double Encryption - Triple Encryption - CDMF Key Shortening – Whitening

Unit IV
Pseudo-Random-Sequence Generators and Stream Ciphers – RC4 - SEAL - Feedback with Carry Shift Registers - Stream Ciphers Using FCSRs - Nonlinear-Feedback Shift Registers - System-Theoretic Approach to Stream-Cipher Design - Complexity-Theoretic Approach to Stream-Cipher Design - N- Hash - MD4 - MD5 - MD2 - Secure Hash Algorithm (SHA) - OneWay Hash Functions Using Symmetric Block Algorithms - Using Public-Key Algorithms - Message Authentication Codes

Unit V
RSA - Pohlig-Hellman - McEliece - Elliptic Curve Cryptosystems -Digital Signature Algorithm (DSA) - Gost Digital Signature Algorithm - Discrete Logarithm Signature Schemes - Ongchnorr-Shamir - Cellular Automata - Feige-Fiat-Shamir -Guillou-Quisquater - Diffie-Hellman - Station-to-Station Protocol -Shamir's Three-Pass Protocol - IBM Secret-Key Management Protocol - MITRENET - Kerberos - IBM Common Cryptographic Architecture.

Books recommended:
- Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C" John Wiley & Sons, Inc, 2nd Edition, 1996.

- Wenbo Mao, "Modern Cryptography Theory and Practice", Pearson Education, 2004

- AtulKahate, "Cryptography and Network Security", Tata McGrew Hill, 2003.

- William Stallings, "Cryptography and Network Security, Prentice Hall, New Delhi, 2006.

- Bernard Menezes, "Network Security and Cryptography", Cengage Learning, New Delhi, 2010

CYBER FORENSICS, AUDIT AND INVESTIGATION

Course Credits: 4 (3-0-2)   **2CS06**

Unit I
File system: CHS, LBA, HPA, write blockers, Extracting & recovering partitions, MBR, DOS partition table, Extended partition table, RAID; FAT file system: Architecture, File creation, File deletion; NTFS file system: Architecture, File creation, File deletion, Compression, encryption and indexing;

Unit II
Extended file systems: EXT2, EXT3 and EXT4, Architecture, File creation, File deletion and Journaling; Apple File System (APFS); Other Disk structures; Windows and Linux boot process; File system acquisition and recovery

Unit III
Windows Forensic Analysis: Window artifacts, Evidence volatility, System time, Logged on user(s), Open files, MRUs, Network information, Process information, Service information, Windows Registry, Start up tasks, Memory dumping; Document Forensics: PDF structure, PDF analysis, MS Office Document structure and analysis, Macros, Windows thumbnails, Android Thumbnails

Unit IV
Mobile Forensics: SIM Card, Android architecture, Android File System, Android application, Android SDK,Android Debug Bridge, Memory & SIM acquisition; Virtual Machines, Network Forensics; Cyber crime investigation: Pre investigation, SOP for Investigation; Case scenarios: social media crime, Online defacement crime, Email investigation; CDR Analysis

Unit V
Auditing: Internal Audit and IT Audit Function, IT Governance, Frameworks, Standards, and Regulations, Identifying information assets, Risk assessment, Risk management, Types of Auditing, ISO 27001, PCIDSS

Books recommended:
- Computer Evidence - Collection and Preservation.Brown, C.L.T. Course Technology Cengage Learning.

- Guide to Computer Forensics And Investigations Nelson, Bill ; Phillips, Amelia; Enfinger, Frank; Steuat, Christopher Thomson Course Technology.

- Computer Forensics – Computer Crime Scene Investigation.Vacca, John R. Charles RiverMedia

- Bunting, Steve and William Wei. EnCase Computer Forensics: The Official EnCE: EnCaseCertifed Examiner Study Guide. Sybex, 2006

- Incident Response: Computer Forensics, Prosise, Chris, Kevin Mandia, and Matt Pepe, McGraw-Hill, 2014

- IT Security Risk Control Management: An Audit Preparation Plan, Raymond Pompon, Apress 2016

- Carrier, Brian. File System Forensic Analysis. Addison-Wesley Professional

WEB APPLICATION AND PENETRATION TESTING

Course Credits: 4 (3-0-2)   **2CS07**

Unit I
Web Fundamentals – HTML, HTTP 1.0 and 1.1, Client-side scripting, Server-side scripting; Web server architecture - Windows & Linux, IIS and LAMP servers, Network topologies and DMZ

Unit II
Web applications: Introduction to web applications, Web application hacking, Overview of browsers, extensions, and platforms **Tools**: *BeFF, Maltego Usage and documentation*

Unit III
OWASP top 10 most critical web application security risks 2017, Attacks, detection evasion techniques, and countermeasures for the most popular web platforms, including IIS, Apache and countermeasures for common web authentication mechanisms, including password-based, multifactor. Tools: Tenable.io Web App Scanning, Lumin, Container Security, Burp Suite Usage and documentation

Unit IV
Advanced session analysis, hijacking, and fixation techniques, cross-site scripting, SQL injection, classic categories of malicious input, Overlong input (like buffer overflows), canonicalization attacks (like the infamous dot-dot-slash), and meta characters, various SQL injection tools and techniques, stealth-encoding techniques and input validation/ output-encoding countermeasures.
Tools: Metasploit, Wireshark usage and documentation

Unit V
Vuln hub Virtual Machine Exploitations using various learning done during class lecture. VAPT Steps: Target Recon, Scanning and Service Enumeration, Vulnerabilities and Exploitation, Post Exploitation - Owning, Pivoting, Privilege, Issues

Books recommended:
- Learning Nessus for Penetration Testing, by Himanshu Kumar

- The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2ed

- Mastering Modern Web Penetration Testing by Prakhar Prasad

- Burp Suite Essentials by Akash Mahajan

- Rtfm: Red Team Field Manual by Ben Clark

- Practical Network Scanning: Capture network vulnerabilities using standard tools by Ajay Singh Chauhan

- Nmap: Network Exploration and Security Auditing Cookbook by Paulino Calderon Pale

- Blue Team Field Manual (RTFM) by Ben Clark

MALWARE ANALYSIS AND NETWORK SECURITY

Course Credits: 4 (3-0-2)   **2CS08**

Unit I
Goals of Malware Analysis, AV Scanning, Hashing, Finding Strings, Packing and Obfuscation, PE file format, Static, Linked Libraries and Functions, Static Analysis tools, Virtual Machines and their usage in malware analysis, Sandboxing, Basic dynamic analysis, Malware execution, Process Monitoring, Viewing processes, Registry snapshots, Creating fake networks,

Unit II
X86 Architecture- Main Memory, Instructions, Opcodes and Endianness, Operands, Registers, Simple Instructions, The Stack, Conditionals, Branching, Rep Instructions, Disassembly, Global and local variables, Arithematic operations, Loops, Function Call Conventions, C Main Method and Offsets. Portable Executable File Format, The PE File Headers and Sections, IDA Pro, Function analysis, Graphing, The Structure of a Virtual Machine, Analyzing Windows programs, Anti-static analysis techniques, obfuscation, packing, metamorphism, polymorphism.

Unit III
 Live malware analysis, dead malware analysis, analyzing traces of malware, system calls, api calls, registries, network activities. Anti-dynamic analysis techniques, VM detection techniques, Evasion techniques, , Malware Sandbox, Monitoring with Process Monitor, Packet Sniffing with Wireshark, Kernel vs. User-Mode Debugging, OllyDbg, Breakpoints, Tracing, Exception Handling, Patching

Unit IV
Downloaders and Launchers, Backdoors, Credential Stealers, Persistence Mechanisms, Handles, Mutexes, Privilege Escalation, Covert malware launching- Launchers, Process Injection, Process Replacement, Hook Injection, Detours, APC injection, YARA rule based detection

Unit V
Android Malware Analysis: Android architecture, App development cycle, APKTool, APKInspector, Dex2Jar, JD-GUI, Static and Dynamic Analysis, Case studies,

Books recommended:
- "Practical Malware Analysis" by Michael Sikorski and Andrew Honig

- "The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System" Second Edition by Reverend Bill Blunden

- "Rootkits: Subverting the Windows Kernel" by Jamie Butler and Greg Hoglund

- "Practical Reverse Engineering" by Dang, Gazet, Bachaalany

- Windows Malware Analysis Essentials by Victor Marak, Packt Publishing, 2015

- Android Malware and Analysis by Dunham Ken, CRC Press

DISSERTATION I

Course Credits: 16 (0-0-32)   **3CS09**

This is the first part of the major dissertation wherein every student shall be expected to contribute to domain knowledge incrementally. It is expected that the research work should be focused in a particular area for concept, design, implementation and/or analysis. Each student will have to undertake a research work under a supervisor. Research work may be carried out within department or in any other academic / research / industrial / commercial organization under the guidance of the thesis supervisor who must be a faculty member of the department or under a joint supervision including at least one such faculty member. The work will have to be carried out during the 3rd semester of study. The student will have to submit a typewritten or printed report on the work done by him / her according to a schedule to be announced by the department. The project-report should be duly approved by the supervisor concerned and should embody results of research / development work carried out by the student.

Student will be continuously evaluated during the semester in form of Dissertation Progress Seminars. At the end of the semester, assessment of the research work of each student will be made by the board of examiners including supervisors on the basis of a viva-voce examination and the report submitted by the student.

DISSERTATION II

Course Credits: 16 (0-0-32)   **4CS10**

This will be culmination of Dissertation I of semester III. Research work may be carried out within department or in any other academic / research / industrial / commercial organization under the guidance of the thesis supervisor who must be a faculty member of the department or under a joint supervision including at least one such faculty member. The student will have to submit typewritten or printed report on the work done by him / her according to a schedule to be announced by the department. The project-report should be duly approved by the supervisor concerned and should embody results of research / development work carried out by the student.

Student will be continuously evaluated during the semester in form of Dissertation Progress Seminars. At the end of the semester, assessment of the research work of each student will be made by the board of examiners including supervisors on the basis of a viva-voce examination and the report submitted by the student.

Students are required to publish their research work in form of research publication. The result will be declared only after acceptance or publication of full length paper in peer reviewed Conference or Journal.

CLOUD COMPUTING

Course Credits: 4 (3-1-0) 1CS51

Unit I
Overview of Computing Paradigm. Recent trends in Computing: Grid Computing, Cluster Computing, Distributed Computing, Utility Computing. Evolution of cloud computing, Cloud Computing (NIST Model), Properties, Characteristics & Disadvantages. Pros and Cons of Cloud Computing, General Benefits and Architecture, Business Drivers, Main players in the Field, Overview of Security Issues, Cloud computing vs. Cluster computing vs. Grid computing. Role of Open Standards

Unit II
Cloud Computing Architecture: Service Models (XaaS), Deployment Models (Public, Private, Hybrid, Community), IaaS: Introduction to virtualization, Different approaches to virtualization, Hypervisors, Machine Image, Virtual Machine (VM), Resource Virtualization (Server, Storage, Network), Examples (Amazon EC2, Eucalyptus)

Unit III
Platform as a Service (PaaS), Service Oriented Architecture (SOA), Cloud Platform and Management, Google App Engine, Microsoft Azure. Software as a Service (SaaS): Introduction to SaaS, Web services, Web 2.0, Web OS, Case Study on SaaS

Unit IV
Cloud Security: Infrastructure Security, Network level security, Host level security, Application level security, Data security and Storage, Data privacy and security Issues, Jurisdictional issues raised by Data location, Amazon's AWS Identity & Access Management and Security in the Cloud, Authentication in cloud computing, Client access in cloud, Cloud contracting Model, Commercial and business considerations. Case Study on Open Source & Commercial Clouds (Eucalyptus, Microsoft Azure, Amazon Web Service)

Unit V
Analysis, Implementations), Membership (Group Membership List, Failure Detectors, Gossip-Style Membership, best failure detector, Another Probabilistic Failure Detector, Dissemination and suspicion), Grids (Applications, Infrastructures), Data Centre Outage Studies

Books recommended:

- Cloud Computing Bible, Barrie Sosinsky, Wiley-India, 2010

- Cloud Computing, Thomas Earl, Pearson, 2014

- Cloud Computing: Principles and Paradigms, RajkumarBuyya, James Broberg, Andrzej Goscinski, Wiley, 2013

- Cloud Computing: Principles, Systems and Applications, Editors: Nikos Antonopoulos, Lee Gillam, Springer, 2012

- Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Ronald L. Krutz, Russell Dean Vines, Wiley-India, 2010

E COMMERCE

Course Credits: 4 (4-0-0) 1CS52

Unit I
Traditional commerce and E commerce – Internet and WWW – role of WWW – value chains – strategic business and Industry value chains – role of E commerce.

Unit II
Packet switched networks – TCP/IP protocol script – Internet utility programmes , HTML, XML, XAML, SOA – web client and servers – Web client/server architecture – intranet and extranets.

Unit III
Web server – performance evaluation - web server software feature sets – web server software and tools – web protocol – search engines – intelligent agents –EC software – web hosting – cost analysis, Google and Facebook Ads case study

Unit IV
Computer security classification – copy right and Intellectual property – electronic commerce threats – protecting client computers – electronic payment systems – electronic cash – strategies for marketing – sales and promotion – cryptography – authentication.

Unit V
Definition and capabilities – limitation of agents – security – web based marketing – search engines and Directory registration – online advertisements – Portables and info mechanics – website design issues, BotNet and its infrastructure.

Books recommended:

- Ravi Kalakota, " Electronic Commerce", Pearson Education,

- Gary P Schneider "Electronic commerce", Thomson learning & James T Peny Cambridge USA, 2001

- Manlyn Greenstein and Miklos "Electronic commerce" McGraw-Hill, 2002.

- EfraimTurvanJ.Lee, David kug and chung, "Electronic commerce" Pearson Education Asia 2001.

- Brenda Kienew E commerce Business Prentice Hall, 2001.

- E - Commerce : Business, Technology, Society- 2016 Edition 10 by by Kenneth C. Laudon, Pearson Education

NEURAL NETWORKS

Course Credits: 4 (3-0-2) 1CS53

Unit I
Neural network, Human Brain, Models of a Neuron, Neural networks as Directed Graphs, Network Architectures, Knowledge Representation, Artificial Intelligence and Neural Networks. Learning– Error Correction learning, Memory based learning, Hebbian learing

Unit II
Learning: Competitive, Boltzmann learning, Credit Assignment Problem, Memory, Adaption, Statistical nature of the learning process. Single Layer Perceptrons: – Adaptive filtering problem, Unconstrained Organization Techniques, Linear least square filters, least mean square algorithm, learning curves, Learning rate annealing techniques, perception –convergence theorem, Relation between perception and Bayes classifier for a Gaussian Environment

Unit III
Multi Layer Perceptrons – Back propagation algorithm XOR problem, Heuristics, Output representation and decision rule, Computer experiment, feature detection
Back Propagation - back propagation and differentiation, Hessian matrix, Generalization, Cross validation, Network pruning Techniques, Virtues and limitations of back propagation learning, Accelerated convergence, supervised learning

Unit IV
Self Organization Maps: Two basic feature mapping models, Self organization map, SOM algorithm, properties of feature map, computer simulations, learning vector quantization, Adaptive patter classification, Hierarchal Vector quantilizer, contexmel Maps

Unit V
Neuro Dynamics: Dynamical systems, stavility of equilibrium states, attractors, neurodynamical models, manipulation of attractors' as a recurrent network paradigm. Hopfield models and experiments

Books recommended:

- Neural networks A comprehensive foundations, Simon Hhaykin, Pearson Education 2nd Edition 2004

- Artificial neural networks - B.Vegnanarayana Prentice Halll of India P Ltd 2005

- Neural networks in Computer intelligence, Li Min Fu TMH 2003

- Neural networks James A Freeman David M S kapura Pearson Education 2004

DATA MINING

Course Credits: 4 (3-0-2)   1CS54

Unit I
Introduction: Fundamentals of data mining, Data Mining Functionalities, Classification of Data
Mining systems, Data Mining Task Primitives, Integration of a Data Mining System with a Database
or a Data Warehouse System, Major issues in Data Mining.
Data Preprocessing: Need for Preprocessing the Data, Data Cleaning, Data Integration and
Transformation, Data Reduction, Discretization and Concept Hierarchy Generation.

Unit II
Mining Frequent Patterns, Associations and Correlations: Basic Concepts, Efficient and Scalable
Frequent Itemset Mining Methods, Mining various kinds of Association Rules, From Association
Mining to Correlation Analysis, Constraint-Based Association Mining

Unit III
Classification and Prediction: Issues Regarding Classification and Prediction, Classification by
Decision Tree Induction, Bayesian Classification, Rule-Based Classification, Classification by Back
propagation, Support Vector Machines, Associative Classification, Lazy Learners, Other
Classification Methods, Prediction, Accuracy and Error measures, Evaluating the accuracy of a
Classifier or a Predictor, Ensemble Methods

Unit IV
Cluster Analysis Introduction :Types of Data in Cluster Analysis, A Categorization of Major
Clustering Methods, Partitioning Methods, Hierarchical Methods, Density-Based Methods, Grid-
Based Methods, Model-Based Clustering Methods, Clustering High-Dimensional Data, Constraint-
Based Cluster Analysis, Outlier Analysis - Mining Streams, Time Series and Sequence Data: Mining
Data Streams, Mining Time-Series Data, Mining Sequence Patterns in Transactional Databases,
Mining Sequence Patterns in Biological Data, Graph Mining, Social Network Analysis and Multi
relational Data Mining

Unit V
Mining Object, Spatial, Multimedia, Text and Web Data: Multidimensional Analysis and Descriptive
Mining of Complex Data Objects, Spatial Data Mining, Multimedia Data Mining, Text Mining,
Mining the World Wide Web. - Applications and Trends in Data Mining: Data Mining Applications,
Data Mining System Products and Research Prototypes, Additional Themes on Data Mining and
Social Impacts of Data Mining.

Books recommended:

- Data Mining – Concepts and Techniques - Jiawei Han & Micheline Kamber, Morgan
  Kaufmann Publishers, 2nd Edition, 2006.

- Introduction to Data Mining – Pang-Ning Tan, Michael Steinbach and Vipin Kumar, Pearson
  education.

- Data Mining Techniques – Arun K Pujari, University Press

INFORMATION SECURITY AND PRIVACY

Course Credits: 4 (3-1-0)   **1CS55**

Unit I
Passwords, security questions, challenge-response, Cryptographic hash functions, Biometrics, Phishing

Unit II
Web security model, Web authentication and session management, Cross-site request forgery, SQL injection, cross-site scripting, Logic flaws in Web applications, Clickjacking

Unit III
Online tracking, Symmetric encryption, Kerberos, Memory corruption attacks and defenses, Viruses and rootkits.

Unit IV
Spam, Attacks on TCP/IP, DNS, BGP. Denial of service, Worms and botnets, Advance Persistent Threats

Unit V
Firewall and intrusion detection, Public Key Cryptography, SSL and certificates, Anonymity networks, Side channel attacks: acoustics and reflections

Books recommended:

- Network Security (2nd edition) by Kaufman, Perlman, and Speciner -- required textbook!

- Security Engineering by Anderson

- The Art of Intrusion by Mitnick and Simon

- The Shellcoder's Handbook by Koziol et al.

- Secure Programming for Unix and Linux HOWTO by Wheeler

- Network Security Essentials by Stallings

SECURITY ANALYSIS OF PROTOCOLS

Course Credits: 4 (3-1-0)   **1CS56**

Unit I
Introduction: Security protocols, Security properties, Public-key certificates and infrastructures, Cryptographic hash functions, Digital signatures, Security protocol vulnerabilities

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

Unit III
Finite-state checking (Murphi), Infinite-state symbolic analysis (SRI constraint solver), Probabilistic model checking (PRISM)

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

Unit V
Transformations: Transformations on protocols, Safe simplifying transformations, Structural transformations. Formal analysis: Formal definitions of security for symmetric ciphers, Formal model for secure key exchange. Theorem proving - Rank functions, Secrecy of shared key, Authentication.

Books recommended:
- Peter Ryan, Steve Schneider, Michael Goldsmith, Gavin Lowe, Bill Roscoe: Modelling & Analysis of Security Protocols, Addison Wesley.

- Stephen W. Mancini: Automating Security Protocol Analysis, Storming Media.

- Selected papers and online material

BIG DATA ANALYTICS

Course Credits: 4 (3-0-2)   **2CS58**

Unit I
Competitive Advantage Definition: Old and New Notions, the Role of Big Data on Gaining Dynamic, Competitive Advantage, Big Data Driven Business Models, Organizational Challenges. Big Data and Analytics for Government Innovation: Governmental Challenges, Smart City Readiness, Learn to Collaborate, Legal Framework Development

Unit II
Big Data and Education: Massive Digital Education Systems: MOOC Educational Model Clusters, Institutional Advantages and Opportunities from MOOCs, Institutional Challenges from MOOCs. Big Data Driven Business Models: Implications of Big Data, for Customer Segmentation, for Value Proposition, for Channels, on Customer Relationships, on Revenue Stream, on Key Resources and Key Partnerships, Organizational Advantages and Opportunities, Organizational Challenges and Threats.

Unit III
Big Data Governance: Big Data Types, Big Data Maturity Models, TDWI Maturity Model, Analytics Business Maturity Model, Data Flux Data Governance Maturity Model, Gartner Maturity Model, IBM Data Governance Maturity Model, Organizational Challenges Inherent with Governing Big Data, Organizational Benefits of Governing Big Data.

Unit IV
Big Data and Digital Business Evaluation: Digital Business Evaluation Using Big Data, Organizational Advantages and Opportunities, Customer Value Proposition, Customer Segmentation, Channels, Customer Relationship, Organizational Challenges.

Unit V
New Big Data Tools to Drive Innovation, The Hadoop Platform, 1010 DATA Cloud Analytics, Actian Analytics, Cloudera, Models of Big Data Change , Big Data Business Model, The Maturity Phases of Big Data Business Model, Big Data Change Key Issue, Organizational Challenges, Data Acquisition, Information Extraction, Data Integration, Aggregation, and Representation

Books recommended:
- Big Data Analytics with R and Hadoop by Vignesh Prajapati, Packt Publication

- Big Data Bootcamp by David Feinleib, Apress Publication

- Big Data and Analytics by Vincenzo Morabito, Springer

- Data Mining Concepts and Techniques, 3rd Edition, Jiawei Han & Micheline Kamber

MACHINE LEARNING

Course Credits: 4 (3-1-0)   **2CS59**

Unit I

Introduction: Basic definitions, types of learning, hypothesis space and inductive bias, evaluation, cross-validation. Linear regression, Decision trees, overfitting

Unit II

Instance based learning, Feature reduction, Collaborative filtering based recommendation. Probability and Bayes learning.

Unit III

Logistic Regression, Support Vector Machine, Kernel function and Kernel SVM. Neural network:Perceptron, multilayer network, backpropagation, introduction to deep neural network.

Unit IV

Computational learning theory, PAC learning model, Sample complexity, VC Dimension, Ensemble learning.

Unit V

Clustering: k-means, adaptive hierarchical clustering, Gaussian mixture model.

Books recommended:

- Machine Learning. Tom Mitchell. First Edition, McGraw- Hill, 1997

- Introduction to Machine Learning Edition 2, by Ethem Alpaydin

- C. Bishop, "Pattern Recognition and Machine Learning, Springer", 2006.

- Shai Shalev-Shwartz, Shai Ben-David, "Understanding Machine Learning: From

- Theory to Algorithms", Cambridge University Press, 2014.

CLOUD COMPUTING AND SECURITY

Course Credits: 4 (3-1-0)   **2CS60**

Unit I

Security Concepts: Confidentiality, privacy, integrity, authentication, non-repudiation, availability, access control, Concepts implementation and relevance in the cloud computing, and their importance in PaaS, IaaS and SaaS. e.g. User authentication in the cloud; Relevant cloud security design principles; least privilege, separation of duties, Defence in Depth, Fail Safe, Economy of Mechanism, Complete Mediation, Open Design, Least Common Mechanism, Weakest Link.

Unit II

Cloud Data Security, Cloud Data Life Cycle; Create, Store, Use, Share, Archive, Destroy, Cloud Storage Architectures; Volume Storage, Object based storage, databases, Content Delivery Network (CDN), Cloud Data Security Foundation Strategies; Encryption, Masking, Obfuscation, Anonymization, Tokenization, Security Information and Event Management, Egress Monitoring (DLP)

Unit III

Shared Cloud Platforms Risks and Responsibilities, Cloud Computing Risks by Deployment and service model, Cloud Attack Surface, Threats by deployment model, Cloud Security Policy Implementation issues and Decomposition, NIST 33 Security Principles, Cloud Penetration Testing; Legal and ethical implications, The three pre-test phases, Usage of various tools including Tenable.io (Vulnerability Management, Web Application Scanning & Container Security) and other penetration testing tools.

Unit IV

Cloud Secure Software Development Life Cycle, ISO/IEC 27034-1 Standards for Secure Application, Single Sign On (SSO), Federated Identity Management, Federation Standards, Multifactor Authentication, Cloud Application Architecture; Secure APIs, Tenancy Separation, Cryptography, Sandboxing, Application Virtualization, Runtime Application Self Protection (RASP)

Unit V

VM Life Cycle; Overwriting, Degaussing, Destruction, Record Retention, Data Remanence, Virtualization Security Management, Virtual Threats, Hypervisor Risks, Increased Denial of Service Risks, VM Security Recommendations, Storage Operations, Physical and Logical Isolation, Basic Operational Application Security, Threat Modelling, Application Testing Methods, Change and Configuration Management, Business Continuity and Disaster Recovery, Incident Response, NIST Special Publication 800-61, Responsibility, ownership of data, Right to penetration test, local law where data is held, Examination of modern Security Standards (e.g. PCIDSS, ISO 27001)

Books recommended:
- Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance" O'Reilly Media; 1 edition, 2009.

- Ronald L. Krutz, Russell Dean Vines, "Cloud Security", 2010.

- John Rittinghouse, James Ransome, "Cloud Computing" CRC Press; 1 edition, 2009.

- J.R. ("Vic") Winkler, "Securing the Cloud" Syngress, 2011.

- Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing".

- Vmware "VMware Security Hardening Guide" White Paper, June 2011

- Cloud Security Alliance 2010, "Top Threats to Cloud Computing" Microsoft 2013.

- Evelyn Brown NIST "Guide to Security for Full Virtualization Technologies", 2011.

INTRODUCTION TO EVOLUTIONARY COMPUTING

Course Credits: 4 (4-0-0)   **2CS61**

Unit I
Introduction, Inspiration from Biology (Darwinian evolution, genetics)
Evolutionary Algorithms: Components, representation, evaluation function, population, parent selection, variation operators, replacement, Initialisation, termination. Knapsack problem

Unit II
Genetic Algorithms: Representation, Mutation, Recombination, Population, Parent selection, Types of survivor selection, Example: Scheduling problem

Unit III
Evolutionary Strategies, Evolutionary Programming,
Example application: Ackley function, evolving checkers players

Unit IV
Genetic Programming: Representation, Mutation, Recombination, Population, Parent selection, Types of survivor selection, Examples

Unit V
Classifier Systems: ZCS: A ``Zeroth Level'' Classifier System, XCS, Extensions, Example: Modelling financial market traders

Books recommended:
- A.E. Eiben and J.E. Smith, Introduction to Evolutionary Computing

INTERNET OF THINGS AND SECURITY

Course Credits: 4 (4-0-0)   **2CS62**

Unit I

Internet of Things (IoT) Introduction, Sensing, Actuation, Basics of Networking, Communication Protocols, Sensor Networks, Machine-to-Machine Communications

Unit II

Interoperability in IoT, Introduction to Arduino Programming, Integration of Sensors and Actuators with Arduino

Unit III

Introduction to Python programming, Introduction to Raspberry Pi, Implementation of IoT with Raspberry Pi

Unit IV

Introduction to SDN, SDN for IoT, Data Handling and Analytics, Cloud Computing, Sensor-Cloud

Unit V

Fog Computing, Smart Cities and Smart Homes, Connected Vehicles, Smart Grid, Industrial IoT Case Study: Agriculture, Healthcare, Activity Monitoring

Books recommended:
- The Internet of Things: Enabling Technologies, Platforms, and Use Cases", by Pethuru Raj and Anupama C. Raman (CRC Press)

- Internet of Things: A Hands-on Approach", by Arshdeep Bahga and Vijay Madisetti (Universities Press)

- Research Papers