I. K. Gujral Punjab Technical University, Jalandhar

Study Scheme and Syllabus - 2020

of

Master of Technology

Computer Science Engineering (Cyber Security)

- **Eligibility: B.E. / B. Tech. (CSE/ IT/ Software Engg./ Computer Engg./ Software Systems/ Information Security/ Cyber Security/ Computational Engg./ Machine learning) with atleast 50% (45% in case of candidate belonging to reserved category).**

SEMESTER - 1

Sem	Course Code	Course Name	L	T	P	Hrs	Internal	External	Total	Credits
1	**MTCy-101-20**	Mathematical Foundations of Computer Science	3	0	0	3	40	60	100	3
1	**MTCy-102-20**	Advanced Data Structures	3	0	0	3	40	60	100	3
1	**MTCy-PE ***	Program Elective – 1	3	0	0	3	40	60	100	3
1	**MTCy-PE ****	Program Elective – 2	3	0	0	3	40	60	100	3
1	**MTCy-111-20**	Advanced Data Structures LAB	0	0	4	4	60	40	100	2
1	**MTCy-112-20**	Elective based LAB	0	0	4	4	60	40	100	2
1	**MTEC-RM1-20**	Research Methodology and IPR	2	0	0	2	40	60	100	2
1	**MTEC-AU1-20**	Audit Course 1	0	0	0	0	40	60	100	0
		Total	**14**	**0**	**8**	**22**	**360**	**440**	**800**	**18**

SEMESTER - 2

Sem	Course Code	Course Name	L	T	P	Hrs	Internal	External	Total	Credits
2	**MTCy-103-20**	Malware Analysis & Reverse Engg.	3	0	0	3	40	60	100	3
2	**MTCy-104-20**	Soft Computing	3	0	0	3	40	60	100	3
2	**MTCy-PE *****	Program Elective – 3	3	0	0	3	40	60	100	3
2	**MTCy-PE ******	Program Elective – 4	3	0	0	3	40	60	100	3
2	**MTCy-113-20**	Malware Analysis & Reverse Engg LAB	0	0	4	4	60	40	100	2
2	**MTCy-114-20**	Elective Based LAB	0	0	4	4	60	40	100	2
2	**MTCy-MP1-20**	Mini Project	0	0	4	4	60	40	100	2
2	**MTAI-AU2-20**	Audit Course 2	0	0	0	0	40	60	100	0
		Total	**12**	**0**	**12**	**24**	**380**	**420**	**800**	**18**

I. K. Gujral Punjab Technical University, Jalandhar

SEMESTER-3

Sem	Course Code	Course Name	L	T	P	Hrs	Internal	External	Total	Credits
3	**MTCy-PE $**	Program Elective-V	3	0	0	3	40	60	100	3
3	**MTCy-OE1-20**	Open Elective	3	0	0	3	40	60	100	3
3	**MTCy-DS1-20**	Dissertation Phase-I	0	0	20	20	60	40	100	10
		Total	**6**	**0**	**20**	**26**	**140**	**160**	**300**	**16**

SEMESTER-4

Sem	Course Code	Course Name	L	T	P	Hrs	Internal	External	Total	Credits
4	**MTCy-DS2-20**	Dissertation Phase-II	**6**	**0**	**20**	**20**	**60**	**40**	**100**	**16**
		Total				**68**	**960**	**1060**	**2000**	**68**

PROGRAMME ELECTIVE COURSES

Programme Elective-I	**MTCy-PE ***	**MTCy-PE1-20** System and Network Security	**MTCy-PE2-20** Ethical Hacking	**MTCy-PE3-20** Intrusion Detection
Programme Elective-II	**MTCy-PE ****	**MTCy-PE4-20** Security Assessment & Risk Analysis	**MTCy-PE5-20** Secure Software Design & Enterprise Computing	**MTCy-PE6-20** Advanced Machine Learning
Programme Elective-III	**MTCy-PE*****	**MTCy-PE7-20** Cryptography	**MTCy-PE8-20** Steganography & Digital Watermarking	**MTCy-PE9-20** Information Theory & Coding
Programme Elective-IV	**MTCy-PE******	**MTCy-PE10-20** Secure Coding	**MTCy-PE11-20** Data Encryption & Compression	**MTCy-PE12-20** Biometrics
Programme Elective-V	**MTCy-PE $**	**MTCy-PE13-20** Blockchain Technology	**MTCy-PE14-20** Data Security and Access Control	**MTCy-PE15-20** Big Data Analytics

OPEN ELECTIVES:

MTAI-OE1-18 Cost Management of Engineering Projects
MTAI-OE2-18 Business Analytics
MTAI-OE3-18 Industrial Safety
MTAI-OE4-18 Operations Research
MTAI-OE5-18 Composite Materials
MTAI-OE6-18 Waste to Energy

AUDIT COURSES I & II

MTA101-18 English for Research Paper Writing
MTA102-18 Disaster Management
MTA103-18 Sanskrit for Technical Knowledge
MTA104-18 Value Education
MTA105-18 Constitution of India
MTA106-18 Pedagogy Studies
MTA107-18 Stress Management by Yoga
MTA108-18 Personality Development through Life Enlightenment Skills

I. K. Gujral Punjab Technical University, Jalandhar

M. Tech (Cyber Security)

FIRST SEMESTER

Course Code	**MTCyS-101-20**
Course Name	**Mathematical Foundations of Computer Science**
Credits	**3**
Pre Requisites	**Discrete Mathematics**

COURSE OBJECTIVE

- To understand the mathematical fundamentals that is prerequisites for a variety of courses like Data mining, Network protocols, analysis of Web traffic, Computer security, Software engineering, Computer architecture, operating systems, distributed systems, Bioinformatics, Machine learning.
- To develop the understanding of the mathematical and logical basis to many modern techniques in in for technology like machine learning, programming language design, and concurrency.
- To study various sampling and classification problems.

COURSE OUTCOMES

- After completion of course, students would be able to:
- To understand the basic notions of discrete and continuous probability.
- To understand the methods of statistical inference, and the role that sampling distributions play in those methods.
- To be able to perform correct and meaningful statistical analyses of simple to moderate complexity.

Syllabus Contents:

Unit 1:

Probability mass, density, and cumulative distribution functions, Parametric families of distributions, Expected value, variance, conditional expectation, Applications of the univariate and multivariate Central Limit Theorem, Probabilistic inequalities, Markov chains

Unit 2:

Random samples, sampling distributions of estimators, Methods of Moments and Maximum Likelihood

Unit 3:

Statistical inference, Introduction to multivariate statistical models: regression and classification problems, principal components analysis, The problem of overfitting model assessment.

Unit 4:

Graph Theory: Isomorphism, Planar graphs, graph colouring, hamilton circuits and euler cycles. Permutations and Combinations with and without repetition. Specialized techniques to solve combinatorial enumeration problems.

Unit 5:

Computer science and engineering applications Data mining, Network protocols, analysis of Web traffic, Computer security, Software engineering, Computer architecture, operating systems, distributed systems, Bioinformatics, Machine learning.

Unit 6:

Recent Trands in various distribution functions in mathmatical field of computer science for varying fields like bioinformatic, soft computing, and computer vision.

Text books:

1. Introduction to Automata Theory, Languages and Computations – J.E. Hopcroft, & J.D. Ullman , Pearson Education Asia.
2. Discrete Mathematical structures with application to Computer Science – J.P. Tremblay and R. Manohar.
3. Cryptography and Network Security, William Stallings.(Second Edition)Pearson Education Asia.

Reference books:

1. Introduction to languages and theory of computation – John C. Martin (MGH)
2. Introduction to Theory of Computation – Michael Sipser (Thomson Nrools/Cole)
3. Cryptanalysis of number theoretic Cyphers, Samuel S. WagstaffJr.Champan& Hall/CRC Press 2003
4. Network Security: The Complete Reference by Roberta Bragg, Mark Phodes –Ousley, Keith Strassberg Tata McGraw-Hill.

I. K. Gujral Punjab Technical University, Jalandhar

Course Code	**MTCyS-102-20**
Course Name	**Advanced Data Structures**
Credits	**3**
Pre Requisites	**UG level course in Data Structures**

COURSE OBJECTIVE

- The student should be able to choose appropriate data structures, understand the ADT/libraries, and use it to design algorithms for a specific problem.
- Students should be able to understand the necessary mathematical abstraction to solve problems.
- To familiarize students with advanced paradigms and data structure used to solve algorithmic problems.
- Student should be able to come up with analysis of efficiency and proofs of correctness

COURSE OUTCOMES

After completion of course, students would be able to:

- Analyze the complexity/performance of different algorithms.
- Determine the appropriate data structure for solving a particular set of problems.
- Categorize the different problems in various classes according to their complexity.
- Students should have an insight of recent activities in the field of the advanced data structure.

Syllabus Contents:

Unit 1:
Sorting: Review of various sorting algorithms, topological sorting Graph: Definitions and Elementary Algorithms: Shortest path by BFS, shortest path in edge-weighted case (Dijkasra's), depth-first search and computation of strongly connected components, emphasis on correctness proof of the algorithm and time/space analysis, example of amortized analysis.

Unit 2:
Matroids: Introduction to greedy paradigm, algorithm to compute a maximum weight maximal independent set. Application to MST. Graph Matching: Algorithm to compute maximum matching. Characterization of maximum matching by augmenting paths, Edmond's Blossom algorithm to compute augmenting path.

Unit 3:
Flow-Networks: Maxflow-mincut theorem, Ford-Fulkerson Method to compute maximum flow, Edmond-Karp maximum-flow algorithm. Matrix Computations: Strassen's algorithm and introduction to divide and conquer paradigm, inverse of a triangular matrix, relation between the time complexities of basic matrix operations, LUP-decomposition.

Unit 4:
Shortest Path in Graphs: Floyd-Warshall algorithm and introduction to dynamic programming paradigm. More examples of dynamic programming. Modulo Representation of integers/polynomials: Chinese Remainder Theorem, Conversion between base-representation and modulo-representation. Extension to polynomials. Application: Interpolation problem. Discrete Fourier Transform (DFT): In complex field, DFT in modulo ring. Fast Fourier Transform algorithm. Schonhage-Strassen Integer Multiplication algorithm.

Unit 5:
Linear Programming: Geometry of the feasibility region and Simplex algorithm. NP-completeness: Examples, proof of NP-hardness and NP-completeness. One or more of the following topics based on time and interest Approximation algorithms, Randomized Algorithms, Interior Point Method, Advanced Number Theoretic Algorithm.

Unit 6:
Recent Trands in problem solving paradigms using recent searching and sorting techniques by applying recently proposed data structures.

Textbooks

1. Fundamentals of data structures in C++ Sahni, Horowitz, Mehatha, Universities Press.
2. Introduction to Algorithms by Cormen, Leiserson, Rivest, Stein.
3. The Design and Analysis of Computer Algorithms by Aho, Hopcroft, Ullman.
4. Algorithm Desig by Kleinberg and Tardos.

References

1. Design methods and analysis of Algorithms, SK Basu, PHI.
2. Data Structures & Algorithm Analysis in C++, Mark Allen Weiss, Pearson Education.
3. Fundamentals of Computer Algorithms, 2nd Edition, Ellis Horowitz, SartajSahni, SanguthevarRajasekaran, Universities Press.

Course Code	**MTEC-RM1-20**
Course Name	**Research Methodology and IPR**
Credits	**3**

COURSE OBJECTIVE

To enable student to acquire knowledge of research process: gather data, implement the proposed work and collect the results and publish them.

COURSE OUTCOMES

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

- Understand research problem formulation.
- Analyze research related information 0 Follow research ethics

- Understand that today's world is controlled by Computer, Information Technology, but tomorrow world will be ruled by ideas, concept, and creativity.
- Understanding that when IPR would take such important place in growth of individuals & nation, it is needless to emphasis the need of information about Intellectual Property Right to be promoted among students in general & engineering in particular.
- Understand that IPR protection provides an incentive to inventors for further research work and investment in R & D, which leads to creation of new and better products, and in turn brings about, economic growth and social benefits.

Syllabus Contents:

Unit 1:
Meaning of research problem, Sources of research problem, Criteria Characteristics of a good research problem, Errors in selecting a research problem, Scope and objectives of research problem. Approaches of investigation of solutions for research problem, data collection, analysis, interpretation, Necessary instrumentations

Unit 2:
Effective literature studies approaches, analysis Plagiarism, Research ethics

Unit 3:
Effective technical writing, how to write report, Paper Developing a Research Proposal, Format of research proposal, a presentation and assessment by a review committee

Unit 4:
Nature of Intellectual Property: Patents, Designs, Trade and Copyright. Process of Patenting and Development: technological research, innovation, patenting, development. International Scenario: International cooperation on Intellectual Property. Procedure for grants of patents, Patenting under PCT.

Unit 5:
Patent Rights: Scope of Patent Rights. Licensing and transfer of technology. Patent information and databases. Geographical Indications.

Unit 6:
New Developments in IPR: Administration of Patent System. New developments in IPR; IPR of Biological Systems, Computer Software etc. Traditional knowledge Case Studies, IPR and IITs.

References:

1. Stuart Melville and Wayne Goddard, "Research methodology: an introduction for science & engineering students'"
2. Wayne Goddard and Stuart Melville, "Research Methodology: An Introduction"
3. Ranjit Kumar, 2nd Edition , "Research Methodology: A Step by Step Guide for beginners".
4. Halbert, "Resisting Intellectual Property", Taylor & Francis Ltd, 2007.
5. Mayall , "Industrial Design", McGraw Hill, 1992.

6. Niebel , “Product Design”, McGraw Hill, 1974.
7. Asimov, “Introduction to Design”, Prentice Hall, 1962.
8. Robert P. Merges, Peter S. Menell, Mark A. Lemley, “ Intellectual Property in New Technological Age”, 2016.
9. T. Ramappa, “Intellectual Property Rights Under WTO”, S. Chand, 2008

Course Code	**MTCyS-PE1-20**
Course Name	**System and Network Security**
Credits	**3**

COURSE OBJECTIVE:

The purpose of this course is to provide understanding of the main issues related to security in modern networked computer systems. This covers underlying concepts and foundations of computer security, basic knowledge about security-relevant decisions in designing IT infrastructures, techniques to secure complex systems and practical skills in managing a range of systems, from personal laptop to large-scale infrastructures.

COURSE OUTCOMES:

On completion of this course, students should have gained a good understanding of the concepts and foundations of computer security, and identify vulnerabilities of IT systems. The students can use basic security tools to enhance system security and can develop basic security enhancements in stand-alone applications.

Syllabus Contents:

Unit 1:
Computer Security Concepts- Introduction to Information Security, Introduction to Data and Network Security, Integrity, and Availability, NIST FIPS 199 Standard, Assets and Threat Models, Examples

Unit 2:
Control Hijacking– Attacks and defenses, Buffer overflow and control hijacking attacks. Exploitation techniques and fuzzing- Finding vulnerabilities and exploits Dealing with Legacy code- Dealing with bad (legacy) application code: Sandboxing and Isolation.

Unit 3:
Least privilege, access control, operating system security- The principle of least privilege, Access control concepts, Operating system mechanisms, Unix, Windows, Qmail, Chromium, and Android examples.

Unit 4:
Basic web security model- Browser content, Document object model (DOM), Same-origin policy. Web Application Security- SQL injection, Cross-site request forgery, Cross-site scripting, Attacks and Defenses, Generating and storing session tokens, Authenticating users, The SSL protocol, The lock icon, User interface attacks, Pretty Good Privacy.

Unit 5:

Network Protocols and Vulnerabilities- Overview of basic networking infrastructure and network protocols, IP, TCP, Routing protocols, DNS. Network Defenses- Network defense tools, Secure protocols, Firewalls, VPNs, Tor, I2P, Intrusion Detection and filters, Host-Based IDS vs Network-Based IDS, Dealing with unwanted traffic: Denial of service attacks, Malicious Software.

Unit 6:

Software Security- Malicious Web, Internet Security Issues, Types of Internet Security Issues, Computer viruses, Spyware, Key-Loggers, Secure Coding, Electronic and Information Warfare. Mobile platform security models- Android, iOSMobile platform security models, Detecting Android malware in Android markets.

Unit 7:

Security Risk Management- How Much Security Do You Really Need, Risk Management, Information. Security Risk Assessment: Introduction, Information Security Risk Assessment: Case Studies, Risk Assessment in Practice.

Unit 8:

The Trusted Computing Architecture- Introduction to Trusted Computing, TPM Provisioning, Exact Mechanics of TPM.

Text books and References:

1. William Stallings, Network Security Essentials: Applications and Standards, Prentice Hall, 4th edition, 2010.
2. Michael T. Goodrich and Roberto Tamassia, Introduction to Computer Security, Addison Wesley, 2011.
3. William Stallings, Network Security Essentials: Applications and Standards, Prentice Hall, 4th edition, 2010.
4. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 2001.

Course Code	**MTCyS-PE2-20**
Course Name	**Ethical Hacking**
Credits	**3**

Course Objectives:

Introduces the concepts of Ethical Hacking. Gives the students the opportunity to learn about different tools and techniques in Ethical hacking and security. Practically apply Ethical hacking tools to perform various activities.

Course Outcomes:

I. K. Gujral Punjab Technical University, Jalandhar

After completion of course, students would be able to: Understand the core concepts related to vulnerabilities and their causes. Understand ethics behind hacking and vulnerability disclosure. Appreciate the impact of hacking. Exploit the vulnerabilities related to computer system and networks using state of the art tools and technologies.

Syllabus Contents:

Unit 1:

Ethical hacking process, Hackers behaviour & mindset, Maintaining Anonymity, Hacking Methodology, Information Gathering, Active and Passive Sniffing, Physical security vulnerabilities and countermeasures. Internal and External testing. Preparation of Ethical Hacking and Penetration Test Reports and Documents.

Unit 2:

Social Engineering attacks and countermeasures. Password attacks, Privilege Escalation and Executing Applications, Network Infrastructure Vulnerabilities, IP spoofing, DNS spoofing, Wireless Hacking: Wireless footprint, Wireless scanning and enumeration, Gaining access (hacking 802.11), WEP, WPA, WPA2.

Unit 3:

DoS attacks. Web server and application vulnerabilities, SQL injection attacks, Vulnerability Analysis and Reverse Engineering, Buffer overflow attacks. Client-side browser exploits, Exploiting Windows Access Control Model for Local Elevation Privilege. Exploiting vulnerabilities in Mobile Application

Unit 4:

Introduction to Metasploit: Metasploit framework, Metasploit Console, Payloads, Metrpreter, Introduction to Armitage, Installing and using Kali Linux Distribution, Introduction to penetration testing tools in Kali Linux. Case Studies of recent vulnerabilities and attacks.

Unit 5:

Malware Analysis: Collecting Malware and Initial Analysis, Hacking Malware

Unit 6:

Case study of vulnerability of cloud platforms and mobile platforms & devices.

Books/References:

1. Shon Harris, Allen Harper, Chris Eagle and Jonathan Ness, Gray Hat Hacking: The Ethical Hackers' Handbook, TMH Edition
2. Jon Erickson, Hacking: The Art of Exploitation, SPD
3. Baloch, R., Ethical Hacking and Penetration Testing Guide, CRC Press, 2015.
4. Beaver, K., Hacking for Dummies, 3rded. John Wiley & sons., 2013.
5. Council, Ec. , Computer Forensics: Investigating Network Intrusions and Cybercrime, Cengage Learning, Second Edition, 2010

6. McClure S., Scambray J., and Kurtz G, Hacking Exposed. Tata McGraw-Hill Education, 6the Edition, 2009 5. International Council of E-Commerce Consultants by Learning, Penetration Testing Network and Perimeter Testing Ec-Council/ Certified Security Analyst Vol. 3 of Penetration Testing, Cenage Learning, 2010
7. Davidoff, S. and Ham, J., Network Forensics Tracking Hackers through Cyberspace, Prentice Hall, 2012. 7. Michael G. Solomon, K Rudolph, Ed Tittel, Broom N., and Barrett, D.,Computer, Forensics Jump Start, Willey Publishing, Inc, 2011.

Course Code	**MTCyS-PE3-20**
Course Name	**Intrusion Detection**
Credits	**3**

COURSE OBJECTIVE:

- Compare alternative tools and approaches for Intrusion Detection through quantitative analysis to determine the best tool or approach to reduce risk from intrusion.
- Identify and describe the parts of all intrusion detection systems and characterize new and emerging IDS technologies according to the basic capabilities all intrusion detection systems share.

COURSE OUTCOMES:

After completion of course, students would be able to:

Apply knowledge of the fundamentals and history of Intrusion Detection in order to avoid common pitfalls in the creation and evaluation of new Intrusion Detection Systems. Evaluate the security an enterprise and appropriately apply Intrusion Detection tools and techniques in order to improve their security posture

Syllabus Contents:

Unit 1:

The state of threats against computers, and networked systems-Overview of computer security solutions and why they fail-Vulnerability assessment, firewalls, VPN's -Overview of Intrusion Detection and Intrusion Prevention- Network and Host-based IDS

Unit 2:

Classes of attacks - Network layer: scans, denial of service, penetration- Application layer: software exploits, code injection-Human layer: identity theft, root access-Classes of attackers-Kids/hackers/sop. Hesitated groups-Automated: Drones, Worms, Viruses

Unit 3:

A General IDS model and taxonomy, Signature-based Solutions, Snort, Snort rules, Evaluation of IDS, Cost sensitive IDS.

Unit 4:
Anomaly Detection Systems and Algorithms-Network Behavior Based Anomaly Detectors (rate based)-Host-based Anomaly Detectors-Software Vulnerabilities- State transition, Immunology, Payload Anomaly Detection.

Unit 5:
Attack trees and Correlation of alerts-Autopsy of Worms and Botnets-Malware detection-Obfuscation, polymorphism-Documentvectors.

Unit 6:
Email/IM security issues-Viruses/Spam-From signatures to thumbprints to zero- day detection-Insider Threat issues-Taxonomy-Masquerade and Impersonation- Traitors, Decoys and Deception-Future: Collaborative Security.

References:

1. The Art of Computer Virus Research and Defense, Peter Szor, Symantec Press ISBN 0-321- 30545-3.
2. Crimeware, Understanding New Attacks and Defenses, Markus Jakobsson and Zulfikar Ramzan, Symantec Press, ISBN: 978-0-321-50195-0 2008

Course Code	**MTCyS-PE4-20**
Course Name	**Security Assessment & Risk Analysis**
Credits	**3**

COURSE OBJECTIVE:

Describe the concepts of risk management. Define and differentiate various Contingency Planning components. Integrate the IRP, DRP, and BCP plans into a coherent strategy to support sustained organizational operations. Define and be able to discuss incident response options, and design an Incident Response Plan for sustained organizational operations.

COURSE OUTCOMES:

After completion of course, students would be: Capable of recommending contingency strategies including data backup and recovery and alternate site selection for business resumption planning. Skilled to be able to describe the escalation process from incident to disaster in case of security disaster. Capable of Designing a Disaster Recovery Plan for sustained organizational operations. Capable of Designing a Business Continuity Plan for sustained organizational operations.

Syllabus Contents:

Unit 1:

SECURITY BASICS: Information Security (INFOSEC) Overview: critical information characteristics – availability information states – processing security Countermeasureseducation, training and awareness, critical information characteristics – confidentiality critical information characteristics –

integrity, information states – storage, information states – transmission, security countermeasures-policy, procedures and practices, threats, vulnerabilities.

Unit 2:

Threats to and Vulnerabilities of Systems: definition of terms (e.g., threats, vulnerabilities, risk), major categories of threats (e.g., fraud, Hostile Intelligence Service (HOIS), malicious logic, hackers, environmental and technological hazards, disgruntled employees, careless employees, HUMINT, and monitoring), threat impact areas.

Unit 3:

Countermeasures: assessments (e.g., surveys, inspections), Concepts of Risk Management: consequences (e.g., corrective action, risk assessment), cost/benefit analysis of controls, implementation of cost-effective controls, monitoring the efficiency and effectiveness of controls (e.g., unauthorized or inadvertent disclosure of information), threat and vulnerability assessment.

Unit 4:

Security Planning: directives and procedures for policy mechanism, Risk Management: acceptance of risk (accreditation), corrective actions information identification, risk analysis and/or vulnerability assessment components, risk analysis results evaluation, roles and responsibilities of all the players in the risk analysis process.

Unit 5:

Contingency Planning/Disaster Recovery: agency response procedures and continuity of operations, contingency plan components, determination of backup requirements, development of plans for recovery actions after a disruptive event, development of procedures for off-site processing, emergency destruction procedures, guidelines for determining critical and essential workload, team member responsibilities in responding to an emergency situation

Unit 6:

Policies and Procedures Physical Security Measures: alarms, building construction, cabling, communications centre, environmental controls (humidity and air conditioning), filtered power, physical access control systems (key cards, locks and alarms)

Unit 7:

Personnel Security Practices and Procedures: access authorization/verification (need-to-know), contractors, employee clearances, position sensitivity, security training and awareness, systems maintenance personnel, Administrative Security Procedural Controls: attribution, copyright protection and licensing, Auditing and Monitoring: conducting security reviews, effectiveness of security programs, investigation of security breaches, privacy review of accountability controls, review of audit trails and logs.

I. K. Gujral Punjab Technical University, Jalandhar

Unit 8:

Operations Security (OPSEC): OPSEC surveys/OPSEC planning INFOSEC: computer security – audit, cryptography-encryption (e.g., point-to-point, network, link), cryptography-key management (to include electronic key), Cryptography-strength (e.g., complexity, secrecy, characteristics of the key). Case study of threat and vulnerability assessment

Books/References:

1. Whitman & Mattord, Principles of Incident Response and Disaster Recovery, Course Technology, ISBN: 141883663X
2. (Web Link) http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf

Course Code	**MTCyS-PE5-20**
Course Name	**Secure Software Design & Enterprise Computing**
Credits	**3**

COURSE OBJECTIVE

- To fix software flaws and bugs in varioussoftware.
- To make students aware of various issues like weak random number generation, information leakage, poor usability, and weak or no encryption on data traffic
- Techniques for successfully implementing and supporting network services on an enterprise scale and heterogeneous systems environment.
- Methodologies and tools to design and develop secure software containing minimum vulnerabilities and flaws.

COURSE OUTCOMES

After completion of course, students would be able to:

- Differentiate between various software vulnerabilities
- Software process vulnerabilities for an organization
- Monitor resources consumption in a software
- Interrelate security and software development process

Syllabus Contents:

Unit 1:

Secure Software Design: Identify software vulnerabilities and perform software security analysis, Master security programming practices, Master fundamental software security design concepts, Perform security testing and quality assurance.

I. K. Gujral Punjab Technical University, Jalandhar

Unit 2:

Enterprise Application Development : Describe the nature and scope of enterprise software applications, Design distributed N-tier software application, Research technologies available for the presentation, business and data tiers of an enterprise software application, Design and build a database using an enterprise database system, Develop components at the different tiers in an enterprise system, Design and develop a multi-tier solution to a problem using technologies used in enterprise system, Present software solution

Unit 3:

Enterprise Systems Administration: Design, implement and maintain a directory-based server infrastructure in a heterogeneous systems environment, Monitor server resource utilization for system reliability and availability, Install and administer network services (DNS/DHCP/TerminalServices/Clustering/Web/Email).

Unit 4:

Obtain the ability to manage and troubleshoot a network running multiple services, Understand the requirements of an enterprise network and how to go about managing them.

Unit 5:

Handle insecure exceptions and command/SQL injection, Defend web and mobile applications against attackers, software containing minimum vulnerabilities and flaws.

Unit 6:

Case study of DNS server, DHCP configuration and SQL injection attack.

References:

1. Theodor Richardson, Charles N Thies, Secure Software Design, Jones & Bartlett
2. Kenneth R. van Wyk, Mark G. Graff, Dan S. Peters, Diana L. Burley, Enterprise Software Security, Addison Wesley.

Course Code	**MTCyS-PE6-20**
Course Name	**Advanced Machine Learning**
Credits	**3**

COURSE OBJECTIVE

- To learn the concept of how to learn patterns and concepts from data without being explicitly programmed in various IOT nodes.
- To design and analyze various machine learning algorithms and techniques with a modern outlook focusing on recent advances.

- Explore supervised and unsupervised learning paradigms of machine learning.
- To explore Deep learning technique and various feature extraction strategies.

COURSE OUTCOMES

After completion of course, students would be able to:

- Extract features that can be used for a particular machine learning approach in various IOT applications.
- To compare and contrast pros and cons of various machine learning techniques and to get an insight of when to apply a particular machine learning approach.

Syllabus Contents:

Unit 1:

Supervised Learning (Regression/Classification): Basic methods: Distance-based methods, Nearest-Neighbours, Decision Trees, Naive Bayes Linear models: Linear Regression, Logistic Regression, Generalized Linear Models. Support Vector Machines, Nonlinearity and Kernel Methods. Beyond Binary Classification: Multi-class/Structured Outputs, Ranking

Unit 2:

Unsupervised Learning: Clustering: K-means/Kernel K-means. Dimensionality Reduction: PCA and kernel PCA. Matrix Factorization and Matrix Completion. Generative Models (mixture models and latent factor models)

Unit 3:

Evaluating Machine Learning algorithms and Model Selection, Introduction to Statistical Learning Theory, Ensemble Methods (Boosting, Bagging, Random Forests)

Unit 4:

Sparse Modeling and Estimation, Modeling Sequence/Time-Series Data, Deep Learning and Feature Representation Learning

Unit 5:

Scalable Machine Learning (Online and Distributed Learning) A selection from some other advanced topics, e.g., Semi-supervised Learning, Active Learning, Reinforcement Learning, Inference in Graphical Models, Introduction to Bayesian Learning and Inference

Unit 6:

Recent trends in various learning techniques of machine learning and classification methods for IOT applications. Various models for IOT applications.

References:

1. Kevin Murphy, Machine Learning: A Probabilistic Perspective, MIT Press, 2012
2. Trevor Hastie, Robert Tibshirani, Jerome Friedman, The Elements of Statistical Learning, Springer 2009 (freely available online)
3. Christopher Bishop, Pattern Recognition and Machine Learning, Springer, 2007.

Audit Courses:

Course Code	**MTEC-AU1-18**
Course Name	**English for research paper writing**
Credits	**0**

COURSE OBJECTIVE

This course is to develop skills in effective English writing to communicate the research work

COURSE OUTCOMES

At the end of this course Students will be able to:

- Understand that how to improve your writing skills and level of readability
- Learn about what to write in each section
- Understand the skills needed when writing a Title
- Ensure the good quality of paper at very first-time submission

Syllabus Contents:

Unit 1
Planning and Preparation, Word Order, breaking up long sentences, Structuring Paragraphs and Sentences, Being Concise and Removing Redundancy, Avoiding Ambiguity and Vagueness

Unit 2
Clarifying Who Did What, Highlighting Your Findings, Hedging and Criticising, Paraphrasing and Plagiarism, Sections of a Paper, Abstracts. Introduction

Unit 3
Review of the Literature, Methods, Results, Discussion, Conclusions, The Final Check.

Unit 4
Key skills are needed when writing a Title, key skills are needed when writing an Abstract, key skills are needed when writing an Introduction, skills needed when writing a Review of the Literature.

Unit 5
Skills are needed when writing the Methods, skills needed when writing the Results, skills are needed when writing the Discussion, skills are needed when writing the Conclusions

Unit 6

I. K. Gujral Punjab Technical University, Jalandhar

Useful phrases, how to ensure paper is as good as it could possibly be the first- time submission

Recommended Books :

1. Goldbort R (2006) Writing for Science, Yale University Press (available on Google Books)
2. Day R (2006) How to Write and Publish a Scientific Paper, Cambridge University Press
3. Highman N (1998), Handbook of Writing for the Mathematical Sciences, SIAM. Highman's book.
4. Adrian Wallwork , English for Writing Research Papers, Springer New York Dordrecht Heidelberg London, 2011.

Course Code	**MTEC-AU1-18**
Course Name	**Disaster Management**
Credits	**0**

COURSE OBJECTIVE

This course is to develop skills in helping society during natural disasters and how to manage.

COURSE OUTCOMES

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

- Learn to demonstrate a critical understanding of key concepts in disaster risk reduction and humanitarian response.
- Critically evaluate disaster risk reduction and humanitarian response policy and practice from multiple perspectives.
- Develop an understanding of standards of humanitarian response and practical relevance in specific types of disasters and conflict situations.
- Critically understand the strengths and weaknesses of disaster management approaches, planning and programming in different countries, particularly their home country or the countries they work in

Syllabus Contents:

Unit 1

Introduction: Disaster: Definition, Factors And Significance; Difference Between Hazard And Disaster; Natural And Manmade Disasters: Difference, Nature, Types And Magnitude.

Unit 2

Repercussions Of Disasters And Hazards: Economic Damage, Loss Of Human And Animal Life, Destruction Of Ecosystem. Natural Disasters: Earthquakes, Volcanisms, Cyclones, Tsunamis, Floods, Droughts And Famines, Landslides And Avalanches, Man-made disaster: Nuclear Reactor Meltdown, Industrial Accidents, Oil Slicks And Spills, Outbreaks Of Disease And Epidemics, War And Conflicts.

Unit 3

Disaster Prone Areas In India Study Of Seismic Zones; Areas Prone To Floods and Droughts, Landslides And Avalanches; Areas Prone To Cyclonic And Coastal Hazards With Special Reference To Tsunami; Post-Disaster Diseases And Epidemics.

Unit 4

Disaster Preparedness And Management Preparedness: Monitoring Of Phenomena Triggering A Disaster Or Hazard; Evaluation Of Risk: Application of Remote Sensing, Data From Meteorological And Other Agencies, Media Reports: Governmental And Community Preparedness.

Unit 5

Risk Assessment Disaster Risk: Concept And Elements, Disaster Risk Reduction, Global And National Disaster Risk Situation. Techniques Of Risk Assessment, Global Co-Operation In Risk Assessment And Warning, People's Participation In Risk Assessment. Strategies for Survival.

Unit 6

Disaster Mitigation Meaning, Concept And Strategies Of Disaster Mitigation, Emerging Trends In Mitigation. Structural Mitigation And Non-Structural Mitigation, Programs Of Disaster Mitigation In India.

Recommended Books :

1. R. Nishith, Singh AK, "Disaster Management in India: Perspectives, issues and strategies" New Royal book Company.
2. Sahni, Pardeep Et.Al. (Eds.)," Disaster Mitigation Experiences And Reflections", Prentice Hall Of India, New Delhi.
3. Goel S. L. , Disaster Administration And Management Text And Case Studies" ,Deep & Deep Publication Pvt. Ltd., New Delhi.

Course Code	**MTEC-AU1-18**
Course Name	**Sanskrit For Technical Knowledge**
Credits	**0**

COURSE OBJECTIVE

This course is to develop

- A working knowledge in illustrious Sanskrit, the scientific language in the world
- Learning of Sanskrit to improve brain functioning
- Learning of Sanskrit to develop the logic in mathematics, science & other subjects enhancing the memory power
- The engineering scholars equipped with Sanskrit will be able to explore the huge knowledge from ancient literature

COURSE OUTCOMES

At the end of this course students will be able to

- Understanding basic Sanskrit language
- Ancient Sanskrit literature about science & technology can be understood
- Being a logical language will help to develop logic in students

Syllabus Contents:

Unit 1
Alphabets in Sanskrit, Past/Present/Future Tense, Simple Sentences.
Unit 2
Order, Introduction of roots, Technical information about Sanskrit Literature.
Unit 3
Technical concepts of Engineering-Electrical, Mechanical, Architecture, Mathematics

Recommended Books :

1. "Abhyaspustakam" – Dr.Vishwas, Samskrita-Bharti Publication, New Delhi
2. "Teach Yourself Sanskrit" Prathama Deeksha-Vempati Kutumbshastri, Rashtriya Sanskrit Sansthanam, New Delhi Publication
3. "India's Glorious Scientific Tradition" Suresh Soni, Ocean books (P) Ltd., New Delhi.

Course Code	**MTEC-AU1-18**
Course Name	**Value Education**
Credits	**0**

COURSE OBJECTIVE

This course is to develop

- Value of education and self- development
- Imbibe good values in students
- Let the should know about the importance of character

COURSE OUTCOMES

At the end of this course students will be able to

- Knowledge of self-development
- Learn the importance of Human values
- Developing the overall personality

Syllabus Contents:

Unit 1

Values and self-development –Social values and individual attitudes. Work ethics, Indian vision of humanism, Moral and non- moral valuation. Standards and principles, Value judgements.

Unit 2

Importance of cultivation of values, Sense of duty, Devotion, Self-reliance, Confidence, Concentration, Truthfulness, Cleanliness, Honesty, Humanity, Power of faith, National Unity, Patriotism, Love for nature, Discipline.

Unit 3

Personality and Behavior Development - Soul and Scientific attitude, Positive Thinking. Integrity and discipline, Punctuality, Love and Kindness, Avoid fault Thinking, Free from anger, Dignity of labour, Universal brotherhood and religious tolerance, True friendship, Happiness Vs suffering, love for truth, Aware of self-destructive habits, Association and Cooperation, Doing best for saving nature.

Unit 4

Character and Competence –Holy books vs Blind faith, Self-management and Good health, Science of reincarnation, Equality, Nonviolence ,Humility, Role of Women, All religions and same message, Mind your Mind, Self-control, Honesty, Studying effectively.

Recommended Books:

1. Chakroborty, S.K. "Values and Ethics for organizations Theory and practice", Oxford University Press, New Delhi

Laboratories

Course Code **MTCyS-111-20**
Course Name **Advanced Data structures LAB**
Credits: 02 **Hours: 04**

Syllabus Contents:

Programs may be implemented using JAVA

Expt. 1:

WAP to store k keys into an array of size n at the location computed using a hash function, loc = key % n, where k<=n and k takes values from [1 to m], m>n. To handle the collisions use the following collision resolution techniques:

a. Linear probing
b. Quadratic probing
c. Double hashing/rehashing
d. Chaining

Expt. 2:

WAP for Binary Search Tree to implement following operations:

a. Insertion
b. Deletion
   Delete node with only child
   Delete node with both children
c. Finding an element
d. Finding Min element
e. Finding Max element
f. Left child of the given node
g. Right child of the given node
h. Finding the number of nodes, leaves nodes, full nodes, ancestors, descendants.

Expt. 3:
WAP for AVL Tree to implement following operations: (For nodes as integers)
a. Insertion: Test program for all cases (LL, RR, RL, LR rotation)
b. Deletion: Test Program for all cases (R0, R1, R-1, L0, L1, L-1)
c. Display: using set notation.

Expt. 4:
WAP to implement Red-Black trees with insertion and deletion operation for the given input data as Integers/Strings

Expt. 5:
WAP to implement insertion, deletion, display and search operation in m-way B tree (i.e. a non-leaf node can have at most m children) for the given data as integers.

Expt. 6:
WAP that implements Kruskal‟s algorithm to generate minimum cost spanning tree

Expt. 7:
WAP to perform string matching using Knuth-Morris-Pratt algorithm for pattern matching.

Expt. 8:
WAP to perform string matching using Boyer-Moore algorithm.

Expt. 9:
WAP to implement 2-D range search over computational geometry problem

Expt. 10:
WAP on latest efficient algorithms on trees for solving contemporary problems.

Mini Project:
Student has to do a project assigned from course contents in a group of two or three students. The team will have to demonstrate as well as have to give a presentation of the same.

Course Code	**MTCyS-112-20**
Course Name	**ElectiveBased LAB**
Credits: 02	**Hours: 04**

ELECTIVE – I

System and Network Security

Objectives:
The main objective is to get knowledge in Configuring DNS Server ,Detecting malicious codes and analysing networks through tools ,implementing various Encryption algorithms

Outcomes:

- Students will get the knowledge in detection ,protection of Intrusions ,malicious codes
- It gives an opportunity to students to get awareness on DNS server, webcrawler, encryption the level of security required for a system in Intranet ,Internet ,cellular networks

List of Experiments:
1. Write a procedure to Logon and Logoff to linux in both Text mode and graphical mode.
2. Configure a DNS Server with a domain name of your choice.
3. Configure FTP on Linux Server. Transfer files to demonstrate the working of the same.
4. Detection of Malicious Code in Registry and Task Manager
5. Checking for rootkits existence in windows.

6. Extracting website map using sam spade (any web crawler)
7. Techniques to stop web crawler
8. Sniff the network traffic while performing port scanning using Nmap.
9. Perform port scanning on Metasploitable 2 vulnerable VM
10. Install JCrypt tool (or any other equivalent) and demonstrate Asymmetric, Symmetric crypto algorithm, Hash and Digital/PKI signatures studied in theory Network Security and Management.
11.Write a client-server program where client sends a text message to server and server sends the text message to client by changing the case(uppercase and lowercase) of each character in the message.
12. Write a client-server program to implement following classical encryption techniques: (I) Ceaser cipher (II) Transposition cipher (III) Row substitution cipher (IV) Hill cipher

Ethical Hacking Lab:

Objectives:

1. The aim of the course is to introduce the methodologies framework tools of ethical hacking to get awareness in enhancing the security
2. To get knowledge on various attacks and their detection

Outcomes:

1. Gain the knowledge of the use and availability of tools to support an ethical hack
2. Gain the knowledge of interpreting the results of a controlled attack

List of Experiments:

1. Setup a honey pot and monitor the honey pot on network
2. Write a script or code to demonstrate SQL injection attacks
3. Create a social networking website login page using phishing techniques
4. Write a code to demonstrate DoS attacks
5. Install rootkits and study variety of options
6. Study of Techniques uses for Web Based Password Capturing.
7. Install jcrypt tool (or any other equivalent) and demonstrate Asymmetric, Symmetric Crypto algorithm, Hash and Digital/PKI signatures studied in theory Network Security And Management
8. Implement Passive scanning ,active scanning, session hizaking, cookies extraction using Burp suit tool

Intrusion Detection

List of experiments will be decided by the instructor based on current research trends / ongoing projects.

ELECTIVE – II

Secure Software Design and Enterprise Computing Lab:

Case Study Analysis:

Based on a real-life situation, for example an armed intervention, a stock market crash or a cyber attack, the students are tasked with a strategic analysis of given problem. In particular, the students

are to develop specific criteria and conduct an assessment of the problem as follows:

1. Understanding and documenting types of cyber attacks.
2. Analyzing and mitigating collected data after a cyber attack has occurred.
3. Creating a cyber risk assessment and mitigation Plan.

For case analysis, consider the following proposed process: Read the situation carefully and consider the key issues. Determine which aspects are the most important to consider. For each aspect/area of importance identified, do the following:

4. Identify key/relevant/critical items and compile facts.
5. Identify problems, elements for more in depth analysis and record in comparative matrices.
6. Consider and document the actions that should be taken to correct the particular negative impacts into positive or negligible outcomes.
7. Determine the positive or negative impact that each item will have against one and another by evaluating the effect of these collective impacts. Be sure to discuss the positive and negative influences caused by their collective interactions

Advanced Machine Learning

List of Experiments:

Programs may be implemented using PYTHON

Expt. 1:

Study of platform for Implementation of Assignments. Download the open source software of your interest. Document the distinct features and functionality of the software platform.

Expt. 2:

Supervised Learning – Regression Generate a proper 2-D data set of N points. Split the data set into Training Data set and Test Data set.

i) Perform linear regression analysis with Least Squares Method.
ii) Plot the graphs for Training MSE and Test MSE and comment on Curve Fitting and Generalization Error.
iii) Verify the Effect of Data Set Size and Bias-Variance Trade off.
iv) Apply Cross Validation and plot the graphs for errors.
v) Apply Subset Selection Method and plot the graphs for errors. Describe your findings in each case.

Expt. 3:

Supervised Learning – Classification Implement Naïve Bayes Classifier and K-Nearest Neighbour Classifier on Data set of your choice. Test and Compare for Accuracy and Precision.

Expt. 4:

Unsupervised Learning Implement K-Means Clustering and Hierarchical clustering on proper data set of your choice. Compare their Convergence.

Expt. 5:

Dimensionality Reduction Principal Component Analysis-Finding Principal Components, Variance and Standard Deviation calculations of principal components.

Expt. 6:

Supervised Learning and Kernel Methods Design, Implement SVM for classification with proper data set of your choice. Comment on Design and Implementation for Linearly non-separable Dataset.

Mini Project:

Student has to do a project assigned from course contents in a group of two or three students. The team will have to demonstrate as well as have to give a presentation of the same.

Security Assessment & Risk Analysis Lab

List of experiments will be decided by the instructor based on current research trends / ongoing projects.