

COURSE STRUCTURE

(Applicable for the Batch admitted from the Academic Year 2018-19 onwards)

I YEAR

I SEMESTER

Group Code	Group	Subject	L	T	P	Credits
	PC 1	Advanced Data Structures	3	-	-	3
	PC 2	Mathematical Foundations of Cryptography	3	-	-	3
	PSE 1	Program Specific Elective 1	3	-	-	3
	PSE 2	Program Specific Elective 2	3	-	-	3
	Laboratory 1	Advanced Data Structures Lab	-	-	4	2
	Laboratory 2	Based on Program Specific Electives 1	-	-	4	2
	PW	Research Methodology & IPR	2	-	-	2
	Audit 1	Audit Course 1	2	-	-	0
		TOTAL	16	0	8	18

Program Specific Elective 1

1. Information Security
2. Distributed Trust or Block chain Technology
3. Ethical Hacking

Program Specific Elective 2

1. Web & Database Security
2. Mobile Application Security
3. Social Media Security

I YEAR

II SEMESTER

Group Code	Group	Subject	L	T	P	Credits
	PC 3	Advanced Algorithms	3	-	-	3
	PC 4	Systems and Network Security	3	-	-	3
	PSE 3	Program Specific Elective 3	3	-	-	3
	PSE 4	Program Specific Elective 4	3	-	-	3
	Laboratory 3	Systems and Network Security Lab	-	-	4	2
	Laboratory 4	Based on Program Specific Electives 4	-	-	4	2
	PW	MINI PROJECT with Seminar	-	-	4	2
	Audit 2	Audit Course 2	2	-	-	0
		TOTAL	14	0	12	18

Program Specific Elective 3

1. Cloud Computing Security
2. Privacy preserving Information Processing
3. Computer Security & Audit Assurance

Program Specific Elective 4

1. Cyber Crime Investigation & Digital Forensics
2. Data Analytics for Fraud Detection
3. Digital Watermarking and Steganography

II YEAR**I SEMESTER**

Group Code	Group	Subject	L	T	P	Credits
	PSE 5	Program Specific Elective 5	3	-	-	3
	OEC	Open Elective	3	-	-	3
	PW	Project/ Dissertation Phase – I	-	-	20	10
		TOTAL	6	0	20	16

Program Specific Elective 5

1. Ad hoc and Sensor Networks
2. Cyber laws and Security Policies
3. Internet of Things

II YEAR**II SEMESTER**

Group Code	Group	Subject	L	T	P	Credits
	PW	Project/ dissertation Phase - II	-	-	32	16
		TOTAL	0	0	32	16

AUDIT COURSES 1 & 2

- 1) English for Research Paper Writing
- 2) Disaster Management
- 3) Professional Ethics
- 4) Value Education
- 5) Constitution of India
- 6) Soft Skills
- 7) Stress Management by YOGA
- 8) Personality Development through Life Enlightenment Skills

OPEN ELECTIVES

- 1) Business Analytics
- 2) Industrial Safety
- 3) Operations Research
- 4) Cost Management of Engineering Projects
- 5) Composite Materials
- 6) Energy from Waste
- 7) Power from Renewable Energy Sources

ADVANCED DATA STRUCTURES

Prerequisites

1. A course on “ Data Structures”

Objectives

1. Introduces the heap data structures such as leftist trees, binomial heaps, fibonacci and min-max heaps
2. Introduces a variety of data structures such as disjoint sets, hash tables, search structures and digital search structures

Outcomes

1. Ability to select the data structures that efficiently model the information in a problem
2. Ability to understand how the choice of data structures impact the performance of programs
3. Can Design programs using a variety of data structures, including hash tables, search structures and digital search structures

UNIT - I

Heap Structures- Introduction, Min-Max Heaps, Leftist trees, Binomial Heaps, Fibonacci heaps.

UNIT - II

Hashing and Collisions

Introduction, Hash Tables, Hash Functions, different Hash Functions:- Division Method, Multiplication Method, Mid-Square Method, Folding Method, Collisions

UNIT - III

Search Structures- OBST, AVL trees, Red-Black trees, Splay trees,

Multiway Search Trees - B-trees., 2-3 trees

UNIT - IV

Digital Search Structures - Digital Search trees, Binary tries and Patricia, Multiway Tries, Suffix trees, Standard Tries, Compressed Tries

UNIT - V

Pattern matching : Introduction, Brute force, the Boyer –Moore algorithm, Knuth-Morris-Pratt algorithm, Naïve String , Harspool, Rabin Karp

Textbooks

1. Fundamentals of data structures in C++ Sahni, Horowitz, Mehatha, Universities Press.
2. Introduction to Algorithms, TH Cormen, PHI

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, Sartaj Sahni, Sanguthevar Rajasekaran, Universities Press.

MATHEMATICAL FOUNDATIONS OF CRYPTOGRAPHY

Objectives

1. Build a solid mathematical basis to understand foundations of cryptography
2. Formally understand the notions related to security authentication and privacy.
3. Provide a rigorous treatment of the emerging and key subject subarea of CSE - security.

Outcomes

1. Students will gain an understanding of cryptosystems widely used to protect data security on the internet, and be able to apply the ideas in new situations as needed.

UNIT- I

Basic functions of cryptography - Encryption Schemes ,Digital Signatures ,Fault Tolerant Protocols and Zero-Knowledge Proofs

The Computational Model: P , NP , and NP- Completeness, Probabilistic Polynomial Time, Non-Uniform Polynomial Time

UNIT- II

Computational Difficulty : One-Way Functions Definitions, Strong One- Way Functions, Weak

One-Way Functions, Universal One-Way Function, Trapdoor One-Way Permutations Computational Indistinguishability: Definition, Relation to Statistical Closeness, Indistinguishability

by Repeated Experiments, Indistinguishability by Circuits

UNIT - III

Zero-Knowledge Proof Systems:

Zero-Knowledge Proofs, Perfect and Computational Zero-Knowledge, An Example (Graph Isomorphism in PZK) Zero-Knowledge with Respect to Auxiliary Inputs

UNIT - IV

Encryption Schemes: Private-Key versus Public-Key Schemes, The Syntax of Encryption Schemes, Semantic Security, Indistinguishability of Encryptions, Stream--Ciphers, Preliminaries: Block--Ciphers

UNIT- V

Digital Signatures and Message Authentication: Attacks and security, Variants

Constructions of Message Authentication Schemes: Applying a pseudorandom function to the document

Text Books:

1. Oded Goldreich, Foundations of Cryptography (two volumes) Cambridge university Press, 2001, 2004. (Indian print available).

Reference Book:

1. J.Katz, Y.Lindell, Introduction to Modern Cryptography, Chapman Hall, USA 2007.
2. Wen Bo Mao, Modern cryptography - Theory and practice, Prentice Hall, USA, 2003
(Indian edition available)

INFORMATION SECURITY
(Program Specific Elective 1)

Prerequisites

1. A Course on “Computer Networks and a course on Mathematics

Objectives

1. To understand the fundamentals of Cryptography
2. To understand various key distribution and management schemes
3. To understand how to deploy encryption techniques to secure data in transit across data networks
4. To apply algorithms used for secure transactions in real world applications

Outcomes

1. Demonstrate the knowledge of cryptography, network security concepts and applications.
2. Ability to apply security principles in system design.
3. Ability to identify and investigate vulnerabilities and security threats and mechanisms to counter them.

UNIT-I

Security Attacks (Interruption, Interception, Modification and Fabrication), Security Services (Confidentiality, Authentication, Integrity, Non-repudiation, access Control and Availability) and Mechanisms, A model for Internetwork security.

Classical Encryption Techniques, DES, Strength of DES, Differential and Linear Cryptanalysis, Block Cipher Design Principles and Modes of operation, Blowfish, Placement of Encryption Function, Traffic Confidentiality, key Distribution, Random Number Generation.

UNIT-II

Public key Cryptography Principles, RSA algorithm, Key Management, Diffie-Hellman Key Exchange, Elliptic Curve Cryptography.

Message authentication and Hash Functions, Authentication Requirements and Functions, Message Authentication, Hash Functions and MACs Hash and MAC Algorithms SHA-512, HMAC.

UNIT -III

Digital Signatures, Authentication Protocols, Digital signature Standard, Authentication Applications, Kerberos, X.509 Directory Authentication Service.

Email Security: Pretty Good Privacy (PGP) and S/MIME.

UNIT-IV

IP Security:

Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management.

Web Security: Web Security Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET).

UNIT-V

Intruders, Viruses and Worms Intruders, Viruses and related threats Firewalls: Firewall Design Principles, Trusted Systems, Intrusion Detection Systems.

Text Books:

1. Cryptography and Network Security (principles and approaches) by William Stallings Pearson Education, 4th Edition.

Reference Books:

1. Network Security Essentials (Applications and Standards) by William Stallings Pearson Education.
2. Principles of Information Security, Whitman, Thomson.

**DISTRIBUTED TRUST or BLOCK CHAIN TECHNOLOGY
(Program Specific Elective - I)**

Prerequisites

1. Knowledge in security and applied cryptography;
2. Knowledge in distributed databases

Objectives

1. Give an introduction to block chain technology and Cryptocurrency

Outcomes

1. Learn about research advances related to one of the most popular technological areas today.

UNIT- I

Introduction: Block chain or distributed trust, Protocol, Currency, Cryptocurrency, How a Cryptocurrency works, Crowdfunding

UNIT- II

Extensibility of Blockchain concepts , Digital Identity verification , Block chain Neutrality , Digital art , Blockchain Environment

UNIT- III

Blockchain Science :Gridcoin , Folding coin, Blockchain Genomics ,Bitcoin MOOCs

UNIT - IV

Currency ,Token ,Tokenizing ,Campuscoin , Coindrop as a strategy for Public adoption, Currency Mut iplicity , Demurrage currency

UNIT - V

Technical challenges , Business model challenges , Scandals and Public perception , Government Regulations

Textbook :

- 1 . Blockchain Blue print for Economy by Melanie Swan

References :

1. Blockchain Basics: A Non-Technical Introduction in 25 Steps 1st ed. Edition, by Daniel Drescher

ETHICAL HACKING
(Program Specific Elective 1)

Prerequisites

1. A course on “Operating Systems”
2. A course on “Computer Networks”
3. A course on “Network Security and Cryptography”

Objectives

1. The aim of the course is to introduce the methodologies and framework of ethical hacking for enhancing the security.
2. The course includes-Impacts of Hacking; Types of Hackers; Information Security Models; Information Security Program; Business Perspective; Planning a Controlled Attack; Framework of Steps (Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Deliverable and Integration)

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
3. Understand the role of politics, inherent and imposed limitations and metrics for planning of a test
4. Comprehend the dangers associated with penetration testing

UNIT- I

Introduction: Hacking Impacts, The Hacker

Framework: Planning the test, Sound Operations, Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Final Analysis, Deliverable, Integration

Information Security Models: Computer Security, Network Security, Service Security, Application Security, Security Architecture

Information Security Program: The Process of Information Security, Component Parts of Information Security Program, Risk Analysis and Ethical Hacking

UNIT - II

The Business Perspective: Business Objectives, Security Policy, Previous Test Results, Business Challenges

Planning for a Controlled Attack: Inherent Limitations, Imposed Limitations, Timing is Everything, Attack Type, Source Point, Required Knowledge, Multi-Phased Attacks, Teaming and Attack Structure, Engagement Planner, The Right Security Consultant, The Tester, Logistics, Intermediates, Law Enforcement

UNIT - III

Preparing for a Hack: Technical Preparation, Managing the Engagement

Reconnaissance: Social Engineering, Physical Security, Internet Reconnaissance

UNIT - IV

Enumeration: Enumeration Techniques, Soft Objective, Looking Around or Attack, Elements of Enumeration, Preparing for the Next Phase

Exploitation: Intuitive Testing, Evasion, Threads and Groups, Operating Systems, Password Crackers, RootKits, applications, Wardialing, Network, Services and Areas of Concern

UNIT - V

Deliverable: The Deliverable, The Document, Overall Structure, Aligning Findings, Presentation

Integration: Integrating the Results, Integration Summary, Mitigation, Defense Planning, Incident Management, Security Policy, Conclusion

Text Book

1. James S. Tiller, "The Ethical Hack: A Framework for Business Value Penetration Testing", Auerbach Publications, CRC Press

Reference Books

1. EC-Council, "Ethical Hacking and Countermeasures Attack Phases", Cengage Learning
2. Michael Simpson, Kent Backman, James Corley, "Hands-On Ethical Hacking and Network Defense", Cengage Learning

WEB & DATABASE SECURITY
(Program Specific Elective - II)

Objectives

1. Give an Overview of information security
2. Give an overview of Access control of relational databases

Outcomes: Students should be able to

1. Understand the Web architecture and applications
2. Understand client side and service side programming
3. Understand how common mistakes can be bypassed and exploit the application
4. Identify common application vulnerabilities

UNIT - I

The Web Security, The Web Security Problem, Risk Analysis and Best Practices
Cryptography and the Web : Cryptography and Web Security, Working Cryptographic Systems and Protocols, Legal Restrictions on Cryptography, Digital Identification

UNIT - II

The Web's War on Your Privacy, Privacy-Protecting Techniques, Backups and Antitheft, Web Server Security, Physical Security for Servers, Host Security for Servers, Securing Web Applications

UNIT - III

Database Security : Recent Advances in Access Control, Access Control Models for XML, Database Issues in Trust Management and Trust Negotiation, Security in Data Warehouses and OLAP Systems

UNIT - IV

Security Re-engineering for Databases: Concepts and Techniques, Database Watermarking for Copyright Protection, Trustworthy Records Retention, Damage Quarantine and Recovery in Data Processing Systems, Hippocratic Databases: Current Capabilities and

UNIT - V

Future Trends Privacy in Database Publishing: A Bayesian Perspective, Privacy-enhanced Location-based Access Control, Efficiently Enforcing the Security and Privacy Policies in a Mobile Environment

Textbook

1. Web Security, Privacy and Commerce Simson Garfinkel, Gene Spafford, O'Reilly.
2. Handbook on Database security applications and trends Michael Gertz, Sushil Jajodia

COMPUTER SECURITY & AUDIT ASSURANCE
(Program Specific Elective - III)

Objectives

1. State the basic concepts in information systems security, including security technology and principles, software security and trusted systems, and IT security management.
2. Explain concepts related to various cryptographic tools.

Outcomes

A student completing this course is expected to be able to:

1. State the requirements and mechanisms for identification and authentication.
2. Explain and compare the various access control policies and models as well as the assurance of these models.

UNIT - I

System Audit and Assurance – Characteristics of Assurance services , Types of Assurance services , Certified Information system auditor , Benefits of Audits for Organization, COBIT

UNIT - II

Internal Control and Information system Audit - Internal Control , Detective control , Corrective Control , Computer Assisted Audit Tools and Techniques

UNIT - III

Conducting Audit – Standard practices , policies , Audit planning , Risk Assessment , Information gathering techniques , Vulnerabilities , System security testing , conducting Audits for Banks

UNIT - IV

Network Security and Control , Internet Banking Risks and Control , Operating System Risks and Control , Operational Control Overview

UNIT - V

Business Continuity and Disaster Recovery Planning Control – Data backup/storage , Developing appropriate Disaster recovering strategy , Business Impact analysis

TextBooks:

1. Information System Audit and Assurance; D. P. Dube, Ved Prakash Gulati; Tata McGraw-Hill Education, 01-Jan2005
2. Auditing IT Infrastructures for Compliance; Martin Weiss, Michael G. Solomon; Jones & Bartlett Publishers, 10Jul-2015

MOBILE APPLICATION SECURITY
(Program Specific Elective – II)

Prerequisites

Undergraduate level knowledge of computer systems and networks

Objectives

1. Gain in-depth knowledge on mobile security and its relation to the new security based protocols.
2. Apply proactive and defensive measures to counter potential threats, attacks and intrusions.

Outcomes

1. By the end of this course students will be able to learn security based protocols , attacks and intrusions

UNIT-I: Top Mobile Issues and Development Strategies: Top Issues Facing Mobile Devices, Physical Security , Secure Data Storage (on Disk), Strong Authentication with Poor Keyboards , Multiple-User Support with Security, Safe Browsing Environment , Secure Operating Systems, Application Isolation, Information Disclosure, Virus, Worms, Trojans, Spyware, and Malware , Difficult Patching/Update Process, Strict Use and Enforcement of SSL, Phishing , Cross-Site Request Forgery (CSRF), Location Privacy/Security, Insecure Device Drivers, Multifactor Authentication, Tips for Secure Mobile Application Development .

UNIT-II: WAP and Mobile HTML Security :WAP and Mobile HTML Basics , Authentication on WAP/Mobile HTML Sites , Encryption , Application Attacks on Mobile HTML Sites ,Cross-Site Scripting , SQL Injection , Cross-Site Request Forgery , HTTP Redirects , Phishing , Session Fixation , Non-SSL Login , WAP and Mobile Browser Weaknesses , Lack of HTTPOnly Flag Support , Lack of SECURE Flag Support , Handling Browser Cache , WAP Limitations.

UNIT-III: Bluetooth Security: Overview of the Technology , History and Standards , Common Uses , Alternatives , Future , Bluetooth Technical Architecture , Radio Operation and Frequency, Bluetooth Network Topology , Device Identification , Modes of Operation , Bluetooth Stack ,Bluetooth Profiles , Bluetooth Security Features , Pairing , Traditional Security Services in Bluetooth, Security “Non-Features” , Threats to Bluetooth Devices and Networks, Bluetooth Vulnerabilities , Bluetooth Versions Prior to v1.2, Bluetooth Versions Prior to v2.1.

UNIT-IV: SMS Security: Overview of Short Message Service, Overview of Multimedia Messaging Service, Wireless Application Protocol (WAP), Protocol Attacks , Abusing Legitimate Functionality, Attacking Protocol Implementations, Application Attacks , iPhone Safari , Windows Mobile MMS, Motorola RAZR JPG Overflow, Walkthroughs ,Sending PDUs ,Converting XML to WBXML .

UNIT-V Enterprise Security on the Mobile OS: Device Security Options , PIN , Remote , 346 Secure Local Storage , Apple iPhone and Keychain , Security Policy Enforcement ,Encryption ,Full Disk Encryption ,E-mail Encryption , File Encryption , Application Sandboxing, Signing, and Permissions , Application Sandboxing , Application Signing , Permissions , Buffer Overflow Protection ,Windows Mobile , iPhone ,Android ,BlackBerry , Security Feature Summary.

Text Book:

1. “Mobile Application Security”, Himanshu Dwivedi, Chris Clark, David Thiel, TATA McGRAW-Hill.

References:

1. “Mobile and Wireless Network Security and Privacy”, Kami S.Makki,et al, Springer.
2. “Android Security Attacks Defenses”, Abhishek Dubey, CRC Press

SOCIAL MEDIA SECURITY
(Program Specific Elective – II)

Objectives

1. Give introduction about the networks, its use, the need of security

Outcomes

1. Learn about browser's risks
2. Learn about Social Networking, Understands the* risks while using social media. Guidelines for social networking
3. Understand how to secure different web browsers.
4. Understand how an e-mail works does; learn threats involved using an email communication, safety measures while using e-mail.

UNIT - I

Introduction: What is Social Media?, Understanding Social Media, Different Types and Classifications, The Value of Social Media, Cutting Edge Versus Bleeding Edge, The Problems That Come With Social Media, Is Security Really an Issue? Taking the Good With the Bad

UNIT - II

Dark side: Cyber crime , Social Engineering , Hacked accounts , cyberstalking, cyberbullying, predators, phishing, hackers

UNIT - III

Being bold versus being overlooked : Good social media campaigns , Bad social media campaigns, Sometimes it's better to be overlooked , Social media hoaxes, The human factor , Content management, Promotion of social media

UNIT - IV

Risks of Social media Risks of social media , Public embarrassment, Once it's out there, it's out there False information, Information leakage, Retention and archiving, Loss of data and equipment

UNIT - V

Policies and Privacy: Blocking users controlling app privacy , Location awareness , Security : Fake accounts , passwords , privacy and information sharing

Text books:

1. Editors: **Altshuler, Y., Elovici, Y., Cremers, A.B., Aharony, N., Pentland, A.** (Eds.)

Interdisciplinary Impact Analysis of Privacy in Social Networks

Recognizing Your Digital Friends

Encryption for Peer-to-Peer Social Networks

Crowdsourcing and Ethics

Social media security

<https://www.sciencedirect.com/science/article/pii/B97815974998660000>

Prerequisites

1. A Course on “Data Structures”

Objectives

1. It introduces searching and sorting algorithms
2. It introduces the balanced trees

Outcomes

1. Develop the feasible and optimal solutions by using Greedy and dynamic programming
2. Able to design Pattern Matching algorithms

List of Programs

1. Write a program to implement the operations of Skip List
2. Write a program to implement Quick sort
3. Write a program to implement Merge sort
4. Write a program to implement Heap sort
5. Write a program to insert the elements into the Hash table by using Linear Probing
6. Write a program to insert the elements into the Hash table by using Quadratic Probing
7. Write a program implement operations of Binary search tree
8. Write a program to implement the operations of AVL tree
9. Write a program to implement the operations of Red-Black tree
10. Write a program to implement the Pattern Matching algorithms by using Boyer Moore, Brute force and KMP algorithm

INFORMATION SECURITY LAB

Prerequisites

1. A Course on “Computer Networks”

Co-requisite

1. A course on “Network Security and Cryptography”

Objective:

1. To get practical exposure of Cryptography algorithms

Outcome:

1. Get the skill to provide security services like authentication confidentiality to the real systems.
2. Get the knowledge to solve security issues in day to day life.

List of Experiments

1. Perform an Experiment for port scanning with nmap
2. Setup a honeypot and monitor the honipot on the network
3. Instal a jcrpt tool(or any other eqivalent) and demonstrate Asymmetric ,Symmetric crypto algorithm ,Hash and Digital/PKI signatures studied in theory Network security and management
4. Using snort perform realtime traffic analysis and packet logging
5. Generate minimum 10 passwords of length 12 cahacters using open ssl command
6. Perform practical approach to implement Footprinting-Gathering target information using Dmitry-Dmagic,UAtester
7. Write a program to perform encryption and decryption using the following substitution ciphers.
8. Caesar cipher
9. Play fair cipher
10. Hill Cipher
11. Write a program to implement the DES algorithm.
12. Write a program to implement RSA algorithm.
13. Calculate the message digest of a text using the SHA-1 algorithm.
14. Working with sniffers for monitoring network communication (Wireshark).
15. Configuring S/MIME for email communication.
16. Using Snort, perform real time traffic analysis and packet logging.

DISTRIBUTED TRUST OR BLOCKCHAIN TECHNOLOGY

Objective

1. The main objective of this course is to provide the knowledge in implementing Blockchains using hash algorithms and bitcoins generation

Outcome

1. By the end of this course students will be able to learn various Hash Algorithms and generation of Bitcoins.

LIST OF EXPERIMENTS

1. Implement Block hash using SHA-256 algorithm using java code or python code
2. Implement Message authentication using Java code or Python code.
3. Implement MD5 algorithm using Java code or python code
4. Implement RIPEMD-160 algorithm using Java code or python code
5. Implement Whirlpool algorithm using Java code or python code
6. Write a case study how the Bitcoins were generated and implemented .

ETHICAL HACKING

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

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

RESEARCH METHODOLOGIES AND IPR

Objective:

1. Introduce research paper writing and induce paper publication skills.
2. Give the introduction to Intellectual Property Rights

Outcomes:

Gain the sound knowledge of the following important elements:

1. Ability to distinguish research methods
2. Ability to write and publish a technical research paper
3. Ability to review papers effectively
4. IPR and Patent filing

UNIT – I

Introduction:

Objective of Research; Definition and Motivation; Types of Research; Research Approaches; Steps in Research Process; Criteria of Good Research; Ethics in Research.

Research Formulation and Literature Review:

Problem Definition and Formulation; Literature Review; Characteristics of Good Research Question; Literature Review Process.

UNIT – II

Data Collection:

Primary and Secondary Data; Primary and Secondary Data Sources; Data Collection Methods; Data Processing; Classification of Data.

Data Analysis:

Statistical Analysis; Multivariate Analysis; Correlation Analysis; Regression Analysis; Principle Component Analysis; Samplings;

UNIT – III

Research Design:

Need for Research Design; Features of a Good Design; Types of Research Designs; Induction and Deduction.

Hypothesis Formulation and Testing:

Hypothesis; Important Terms; Types of Research Hypothesis; Hypothesis Testing; Z-Test; t-Test; f-Test; Making a Decision; Types of Errors; ROC Graphics.

UNIT – IV

Test Procedures:

Parametric and Non Parametric Tests; ANOVA; Mann-Whitney Test; Kruskal-Wallis Test; Chi-Square Test; Multi-Variate Analysis.

Presentation of the Research Work:

Business Report; Technical Report; Research Report; General Tips for Writing Report; Presentation of Data; Oral Presentation; Bibliography and References; Intellectual Property Rights; Open-Access Initiatives; Plagiarism.

UNIT – V

Law of Patents, Patent Searches, Ownership, Transfer

Patentability – Design Patents – Double Patenting – Patent Searching – Patent Application Process – Prosecuting the Application, Post-issuance Actions, Term and Maintenance of Patents. Ownership Rights – Sole and Joint Inventors – Inventions Made by Employees and Independent Contractors – Assignment of Patent Rights – Licensing of Patent Rights – Invention Developers and Promoters.

Patent Infringement, New Developments and International Patent Law

Direct Infringement – Inducement to Infringe – Contributory Infringement – First Sale Doctrine – Claims Interpretation – Defenses to Infringement – Remedies for Infringement – Resolving an Infringement Dispute – Patent Infringement Litigation. New Developments in Patent Law

Text Books

1. Research Methodology. Methods & Technique : Kothari. C.R.
2. Intellectual Property – Copyrights, Trademarks, and Patents by Richard Stim, Cengage Learning

References

1. Practical Research : planning and Design(8th Edition) – Paul D. Leedy and Jeanne E. Ormrod.
2. A Hand Book of Education Research – NCTE
3. Methodology of Education Research – K.S. Sidhu.
4. Tests, Measurements and Research methods in Behavioural Sciences- A.K. Singh.
5. Statistical Methods- Y.P. Agarwal.
6. Methods of Statistical Ananalysis- P.S Grewal.
7. Fundamentals of Statistics – S.C. Gupta, V.K. Kapoor.
8. Intellectual Property Rights by Deborah E. Bouchoux, Cengage Learning.
9. Managing Intellectual Property – The Strategic Imperative, Second Edition by Vinod V.Sople, PHI Learning Private Limited.

ADVANCED ALGORITHMS**Prerequisites**

1. A course on “Computer Programming & Data Structures”
2. A course on “Advanced Data Structures & Algorithms”

Objectives

1. Introduces the recurrence relations for analyzing the algorithms
2. Introduces the graphs and their traversals.
3. Describes major algorithmic techniques (divide-and-conquer, greedy, dynamic programming, Brute Force , Transform and Conquer approaches) and mention problems for which each technique is appropriate;
4. Describes how to evaluate and compare different algorithms using worst-case, average-case and best-case analysis.
5. Introduces string matching algorithms
6. Introduces linear programming.

Outcomes

1. Ability to analyze the performance of algorithms
2. Ability to choose appropriate data structures and algorithm design methods for a specified application
3. Ability to understand how the choice of data structures and the algorithm design methods impact the performance of programs

UNIT – I

Classification of algorithms, Algorithm Specifications,

Mathematical analysis of Recursive Algorithms: – Introduction to recurrence equations, formulation of recurrence equations, Techniques for solving recurrence equations, Solving recurrence equations, Solving Recurrence Equations using polynomial reduction, Divide and conquer recurrences

UNIT – II

Graphs :– Graph representations, Graph traversals

Brute Force Approaches:- Computational Geometry Problems-Closest pair problem, Convex Hull Problem, Exhaustive Searching- Magic Squares problem, Container Loading problem, Knapsack Problem, Assignment Problem

UNIT – III

Divide and Conquer approach:- Multiplication of long integers, Strassen’s matrix multiplication, Fourier Transform

Greedy algorithms:- Coin change problem, Scheduling problems, knapsack problem, optimal storage on tapes, optimal tree problems, optimal graph problems

UNIT – IV

Transform and Conquer approach :- Matrix operations- Gaussian Elimination method, LU decomposition, Crout’s method of decomposition

Dynamic Programming:- Computing binomial coefficients, Multistage graph problem, Transitive Closure and Warshall algorithm, Floyd warshall all pairs shortest path problem, TSP, Flow shop scheduling algorithm

UNIT – V

String algorithms:- Basic string algorithms, Longest Common Subsequences.

Linear Programming, Graphical method for solving LPP, Simplex method, Minimization problems, Principle of Duality, Max Flow problem

TEXT BOOKS:

1. Design and Analysis of Algorithms, S.Sridhar, OXFORD University Press

REFERENCES :

1. Introduction to Algorithms, second edition, T.H.Cormen, C.E.Leiserson, R.L.Rivest and C.Stein, PHI Pvt. Ltd./ Pearson Education.
2. Fundamentals of Computer Algorithms, Ellis Horowitz, Satraj Sahni and Rajasekharam, Universities Press.
3. Design and Analysis of algorithms, Aho, Ullman and Hopcroft, Pearson education

Prerequisites : Computer Networks , Network Security

Objectives

1. A brief explanation of the objective is to provide knowledge on different types of Intrusions occur at various Network levels , and level of security provisions required when the systems are used at different networks in LAN,WAN

Outcomes

1. Students will get the knowledge in detection, protection of Intrusions.
2. It gives an opportunity to students to get awareness on the level of security required for a system in Intranet ,Internet ,cellular networks

UNIT - I

Detecting System Intrusions : Monitoring Key Files in the System ,Zero Day attacks ,Fullpacket capture devices ,Data correlation ,SEIM, Network-Based Detection of System Intrusions

Preventing System Intrusions :Symptoms of Intrusions ,Security policies , Risk Analysis ,Controlling user Access, Intrusion Prevention capabilities

UNIT - II

Guarding Against Network Intrusions: Traditional Reconnaissance and Attacks, Malicious Software , Defense in Depth, Preventive Measures , Intrusion Monitoring and Detection, Reactive Measures, Network-Based Intrusion Protection

Internet Security : Internet Protocol Architecture,. Internet Threat Model, Defending against Attacks on the Internet , Internet Security Checklist

UNIT - III

Intranet Security: Smartphones and Tablets in the Intranet ,Security ConsiderationsPlugging the Gaps: NAC and AccessControl, Measuring Risk: Audits,. Guardian at the Gate: Authentication,and Encryption ,Wireless Network Security , Shielding the Wire: NetworkProtection,Weakest Link in Security: User Training , Documenting the Network: Change Management

UNIT - IV

Local Area Network Security : Identify Network Threats, Establish Network Access Controls, Risk Assessment, Listing Network Resources, Threats, Security Policies, The Incident-Handling Process, Secure Design Through Network, Access Controls , IDS Defined NIDS: Scope and Limitations, Firewalls , Dynamic NAT Configuration Packet Filtering: IP Filtering Routers, Application-Layer Firewalls: Proxy Servers

UNIT - V

Cellular Network Security: The State of the Art of Cellular Network Security, Cellular Network Attack Taxonomy, Cellular Network Vulnerability Analysis

RFID Security : RFID challenges ,RFID protections

Text Books

1. Network and System Security ,John R Vacca , Second edition , Syngress publications

CLOUD COMPUTING SECURITY
(Program Specific Elective - III)

Objectives

1. Guiding Security design principles for Cloud Computing
2. Be able to understand the legal, security, forensics, personal & data privacy issues within Cloud environment
3. Understand the concepts and guiding principles for designing and implementing appropriate safeguards and countermeasures for Cloud based IT services

Outcomes

1. Approaches to designing cloud services that meets essential Cloud infrastructure characteristics on demand computing, shared resources, elasticity and measuring usage.
2. Design security architectures that assures secure isolation of physical and logical infrastructures
3. Understand the industry security standards, regulatory mandates, audit policies and compliance requirements for Cloud based infrastructures.

UNIT - I

Introduction to cloud – Basic Concepts and Terminology – Concepts and Models of cloud computing – Cloud delivery and deployment models.

UNIT - II

Cloud enablers and security – Internet, Broadband, Data centre and virtualization technologies,

UNIT - III

Web and Multitenant services – Cloud security,

UNIT - IV

Agent threats: Cloud infrastructure mechanisms, Specialized cloud mechanisms,

UNIT - V

Cloud Management and Cloud Security. AWS, Azure and Google case study

References:

1. T. Mather, S. Kumaraswamy, S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Series, 2009.
2. T. Erl, R. Puttini, Z. Mahmood, Cloud Computing: Concepts, Technology & Architecture, Prentice Hall, 2013.
3. The Google file system. In Proceedings of the nineteenth ACM symposium on Operating systems principles (SOSP '03). ACM, New York, NY, USA, 29-43.
4. MapReduce: simplified data processing on large clusters. Commun. ACM 51, 1, 107-113, 2008.
5. Controlling data in the cloud: outsourcing computation without outsourcing control. In Proceedings of the 2009 ACM workshop on Cloud computing security (CCSW '09). ACM, New York, NY, USA, 85-90, 2009.

**PRIVACY PRESERVING INFORMATION PROCESSING
(Program Specific Elective - III)**

Objectives

1. Techniques in protecting data privacy and data security when the data is released to public.

Outcomes

1. By the end of this course student will be able to get knowledge in various data privacy issues and their preventions

UNIT - I

Malware

Exploring Timeline-Based Malware Classification , Screening Smartphone Applications Using Behavioral Signatures .

Authentication and Authorization

Evolving a Secure Internet , Enhancing Click-Draw Based Graphical Passwords Using Multi-Touchon Mobile Phones, Applying DAC Principles to the RDF Graph Data Model

UNIT - II

Network Security/ Cryptography

Extraction of ABNF Rules from RFCs to Enable Automated Test Data Generation , Key Derivation Function: The SCKDF Scheme

UNIT - III

Software Security

Improving Mobile Device Security with Operating System-Level Virtualization, Generating Realistic Application Workloads for Mix-Based Systems for Controllable, Repeatable and Usable Experimentation

UNIT - IV

Privacy Protection

Enforcement of Privacy Requirements ,Towards Security-Enhanced and Privacy-Preserving Mashup Compositions, On Privacy-Preserving Ways to Porting the Austrian eID System to the Public Cloud .

UNIT - V

Risk Analysis and Security Metrics

Using the Conflicting Incentives Risk Analysis Method Performance Analysis of Scalable Attack Representation Models

Security Management/Forensic

Secure Outsourcing: An Investigation of the Fit between Clients and Providers

TEXT BOOKS

1. Security and privacy protection in information processing systems by Lech J. Janczewski, Henry B .Wolfe, Sujeet Sheno

COMPUTER SECURITY & AUDIT ASSURANCE
(Program Specific Elective - III)

Objectives

1. To introduce the fundamental concepts and techniques in computer and network security,
2. an overview of information security and auditing, and to expose students to the latest trend of computer attack and defence

Outcomes

1. Describe fundamental concepts of information security and systems auditing
2. Analyze the latest trend of computer security threats and defence
3. Identify security weaknesses in information systems, and rectify them with appropriate security mechanisms
4. Explain the security controls in the aspects of physical, logical and operational security control

UNIT - I

System Audit and Assurance – Characteristics of Assurance services , Types of Assurances services ,Certified Information system auditor , Benefits of Audits for Organization, COBIT

UNIT - II

Internal Control and Information system Audit - Internal Control, Detective control, Corrective Control ,Computer Assisted Audit Tools and Techniques

UNIT - III

Conducting Audit – Standard practices, policies, Audit planning, Risk Assessment, Information gathering techniques, Vulnerabilities, System security testing, conducting Audits for Banks

UNIT - IV

Network Security and Control ,Internet Banking Risks and Control , Operating System Risks and Control , Operational Control Overview

UNIT - V

Business Continuity and Disaster Recovery Planning Control – Databackup/storage, Developing appropriate Disaster recovering strategy, Business Impact analysis

References:

1. Information System Audit and Assurance; D. P. Dube, Ved Prakash Gulati; Tata McGraw-Hill Education, 01-Jan2005
2. Auditing IT Infrastructures for Compliance; Martin Weiss, Michael G. Solomon; Jones & Bartlett Publishers, 10Jul-2015

**CYBER CRIME INVESTIGATION & DIGITAL FORENSICS
(Program Specific Elective - IV)**

Prerequisites

1. Knowledge of information technology fundamentals (computer hardware, operating systems, applications and networking) is required.

Objectives

1. An introduction to the methodology and procedures associated with digital forensic analysis in a network environment

Outcomes

1. Obtain and analyze digital information for possible use as evidence in civil, criminal or administrative cases.
2. They will learn about the importance of digital forensic principles and procedures, legal considerations, digital evidence controls

UNIT - I

Framework for Digital Forensic Evidence Collection and Processing, Fundamentals of Host Forensics for Microsoft Windows - Kernel and Device driver architecture, registry, auditing and security architecture File system handling - Reconstruction of files and directory structures on the FAT and NTFS

UNIT - II

Fundamentals of Host Forensics for UNIX derivatives - Linux operating system, Kernel and Device drives architecture, Security and audit mechanisms, file system and pseudo file systems, the reconstruction of file and directory structures using UFS and Ext2/3fs as exemplars.

UNIT - III

Forensic Analysis of Database Systems, Database Tampering, Forensic analysis of Database Components, table storage, transaction log, indexes, Forensic recovery for table storage.

UNIT - IV

Network Forensics, investigating logs, network traffic and web attacks, Mobile Device and Wireless Forensics, Anti-Forensics,

UNIT - V

Steganography and Image file Forensics, Email investigation, Investigating Copiers, IVR, Video Surveillance, RFID and Vehicular tracking (GPS) devices, Case studies and Tools.

Text Books/References

1. E. P. Dorothy, Real Digital Forensics for Handheld Devices , Auerback Publications, 2013.
2. J. Sammons, The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, Syngress Publishing, 2012.
3. E. Casey, Handbook of Digital Forensics and Investigation, Academic Press, 2010

4. C. H. Malin, E. Casey and J. M. Aquilina, Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides, Syngress, 2012
5. J. Wiles and A.Reyes, The Best Damn Cybercrime and Digital Forensics Book Period, Syngress, 2007.

DATA ANALYTICS FOR FRAUD DETECTION
(Program Specific Elective - IV)

Objectives

1. Discuss the overall process of how data analytics is applied
2. Discuss how data analytics can be used to better address and identify risks
3. Help mitigate risks from fraud and waste for our clients and organizations

Outcomes

1. Formulate reasons for using data analysis to detect fraud.
2. Explain characteristics and components of the data and assess its completeness.
3. Identify known fraud symptoms and use digital analysis to identify unknown fraud symptoms.
4. Automate the detection process.
5. Verify results and understand how to prosecute fraud

UNIT - I

Introduction: Defining Fraud, Anomalies versus Fraud, Types of Fraud, Assess the Risk of Fraud, Fraud Detection, Recognizing Fraud, Data Mining versus Data Analysis and Analytics, Data Analytical Software, Anomalies versus Fraud within Data, Fraudulent Data Inclusions and Deletions

UNIT - II

The Data Analysis Cycle, Evaluation and Analysis, Obtaining Data Files, Performing the Audit, File Format Types, Preparation for Data Analysis, Arranging and Organizing Data,

Statistics and Sampling, Descriptive Statistics, Inferential Statistics

UNIT - III

Data Analytical Tests : Benford's Law, Number Duplication Test , Z-Score, Relative Size Factor Test, Same-Same-Same Test , Same-Same-Different Test

UNIT - IV

Advanced Data Analytical Tests

Correlation, Trend Analysis, , GEL-1 and GEL-2 , Skimming and Cash Larceny, Billing schemes : and Data Familiarization, , Benford's Law Tests, Relative Size Factor Test , Match Employee Address to Supplier data

UNIT - V

Payroll Fraud , Expense Reimbursement Schemes , Register disbursement schemes

Textbook

1. Fraud and Fraud Detection: A Data Analytics Approach by Sunder Gee , Wiley

DIGITAL WATERMARKING AND STEGANOGRAPHY

(Program Specific Elective - IV)

Objectives

1. To learn about the watermarking models and message coding
2. To learn about watermark security and authentication.
3. To learn about steganography. Perceptual models

Outcomes

1. Know the History and importance of watermarking and steganography
2. Analyze Applications and properties of watermarking and steganography
3. Demonstrate Models and algorithms of watermarking
4. Possess the passion for acquiring knowledge and skill in preserving authentication of Information
5. Identify theoretic foundations of steganography and steganalysis

UNIT - I

Introduction: Information Hiding, Steganography and Watermarking – History of watermarking – Importance of digital watermarking – Applications – Properties – Evaluating watermarking systems.

Watermarking models & message coding: Notation – Communications – Communication based models – Geometric models – Mapping messages into message vectors – Error correction coding – Detecting multi-symbol watermarks.

UNIT - II

Watermarking with side information & analyzing errors: Informed Embedding – Informed Coding – Structured dirty-paper codes - Message errors – False positive errors – False negative errors – ROC curves – Effect of whitening on error rates.

UNIT - III

Perceptual models: Evaluating perceptual impact – General form of a perceptual model – Examples of perceptual models – Robust watermarking approaches - Redundant Embedding, Spread

Spectrum Coding, Embedding in Perceptually significant coefficients

UNIT - IV

Watermark security & authentication: Security requirements – Watermark security and cryptography – Attacks – Exact authentication – Selective authentication – Localization – Restoration.

UNIT - V

Steganography: Steganography communication – Notation and terminology – Information-theoretic foundations of steganography – Practical steganographic methods – Minimizing the embedding impact – Steganalysis

References

1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, “Digital
2. Watermarking and Steganography”, Margan Kaufmann Publishers, New York, 2008.
3. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, “Digital Watermarking”, Margan Kaufmann Publishers, New York, 2003.

4. Michael Arnold, Martin Schmucker, Stephen D. Wolthusen, “Techniques and Applications of Digital Watermarking and Content Protection”, Artech House, London, 2003.
5. Juergen Seits, “Digital Watermarking for Digital Media”, IDEA Group Publisher, New York, 2005.
6. Peter Wayner, “Disappearing Cryptography – Information Hiding: Steganography & Watermarking”, Morgan Kaufmann Publishers, New York, 2002.

SYSTEMS AND NETWORK SECURITY LAB

Objectives

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

Outcomes

1. Students will get the knowledge in detection ,protection of Intrusions ,malicious codes
2. 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

CYBER CRIME INVESTIGATION & DIGITAL FORENSICS LAB

Objectives

1. To provide students with a comprehensive overview of collecting, investigating, preserving, and presenting evidence of cyber crime left in digital storage devices, emails, browsers, mobile devices using different Forensics tools
2. To Understand file system basics and where hidden files may lie on the disk, as well as how to extract the data and preserve it for analysis.
3. Understand some of the tools of e-discovery.
4. To understand the network analysis ,Registry analysis and analyse attacks using different forensics tools

Outcomes

1. Learn the importance of a systematic procedure for investigation of data found on digital storage media that might provide evidence of wrong-doing
2. To Learn the file system storage mechanisms and retrieve files in hidden format
3. Learn the use of computer forensics tools used in data analysis.
4. Learn how to find data that may be clear or hidden on a computer disk, find our the open ports for the attackers through network analysis , Registry analysis.

Experiments

1. **Perform email analysis** using the tools like Exchange EDB viewer , MBOX viewer and View user mailboxes and public folders , Filter the mailbox data based on various criteria, Search for particular items in user mailboxes and public folders
2. **Perform Browser history analysis** and get the downloaded content , history ,saved logins,s earches ,websites visited etc using Foxtton Forensics tool,Dumpzilla .
3. **Perform mobile analysis** in the form of retrieving call logs ,SMS log ,all contacts list using the forensics tool like SAFT
4. **Perfrom Registry analysis** and get boottime logging using process monitor tool
5. **Perform Disk imaging and cloning the** using the X-way Forensics tools
6. **Perform Data Analysis i.e** History about open file and folder, and view folder actions using Lastview activity tool
7. **Perform Network analysis** using the Network Miner tool .
8. **Perform information for incident response** using the crowd Response tool
9. **Perform File type detection using** Autospy tool
10. **Perform Memory capture and analysis** using the Live RAM capture or any forensic tool

DATA ANALYTICS FOR FRAUD DETECTION

Objective

1. The main objective is to perform data analysis and detect fraud activities

Outcome

1. Gain knowledge in performing fraud detection by data analysis using different tools

List Of Experiments

1. **Perform data analysis** i.e history about open file and folder, and view folder actions using last view activity tool
2. **Perform file type detection using** auto spy tool
3. **Perform network analysis** using the network miner tool
4. Create a social networking website login page using phishing techniques
5. Analyse ddos attacks and write code to prevent ddos attacks
6. Analyse sql injection attacks and write code to prevent ddos attacks
7. Analyse buffer overflow attacks and write code to prevent ddos attacks .
8. **Perform memory capture and analysis** using the live ram capture or any forensic tool

DIGITAL WATERMARKING AND STEGANOGRAPHY LAB

Objective

1. The objective of this course is to provide knowledge in implementing watermarking and steganography lab

Outcomes

1. By the end of this course Students will be able to implement watermarking techniques and Steganography techniques using code

List of Experiments

1. Write a code to implement watermarking in the document.
2. Write a code to remove watermarking from the document
3. Write a code to hide the data in image
4. Write a code to hide the photo in plain sight
5. Write a code to hide to implement Information hiding
6. Implement the Hiding the text in image using steganography S-Tool
7. Write a code to retrieve the hidden image from data
8. Write a code to retrieve the hidden text from image
9. Write a code to extract photo from plainsight
10. Write a code to implement encryption using steganography

AD HOC AND SENSOR NETWORKS
(Program Specific Elective - V)

Prerequisites

1. A course on “Computer Networks”
2. A course on “Mobile Computing”

Objectives

1. To understand the concepts of sensor networks
2. To understand the MAC and transport protocols for ad hoc networks
3. To understand the security of sensor networks
4. To understand the applications of adhoc and sensor networks

Outcomes

1. Ability to understand the state of the art research in the emerging subject of Ad Hoc and Wireless Sensor Networks
2. Ability to solve the issues in real-time application development based on ASN.
3. Ability to conduct further research in the domain of ASN

UNIT - I

Introduction to Ad Hoc Networks - Characteristics of MANETs, Applications of MANETs and Challenges of MANETs.

Routing in MANETs - Criteria for classification, Taxonomy of MANET routing algorithms, Topology-based routing algorithms-**Proactive**: DSDV; **Reactive**: DSR, AODV; Hybrid: ZRP; Position-based routing algorithms-**Location Services**-DREAM, Quorum-based; **Forwarding Strategies**: Greedy Packet, Restricted Directional Flooding-DREAM, LAR.

UNIT - II

Data Transmission - Broadcast Storm Problem, **Rebroadcasting Schemes**-Simple-flooding, Probability-based Methods, Area-based Methods, Neighbor Knowledge-based: SBA, Multipoint Relaying, AHBP. **Multicasting**: **Tree-based**: AMRIS, MAODV; **Mesh-based**: ODMRP, CAMP; **Hybrid**: AMRoute, MCEDAR.

UNIT - III

Geocasting: Data-transmission Oriented-LBM; Route Creation Oriented-GeoTORA, MGR.

TCP over Ad Hoc TCP protocol overview, TCP and MANETs, Solutions for TCP over Ad hoc

UNIT - IV

Basics of Wireless, Sensors and Lower Layer Issues

Applications, Classification of sensor networks, Architecture of sensor network, Physical layer, MAC layer, Link layer, Routing Layer.

UNIT - V

Upper Layer Issues of WSN

Transport layer, High-level application layer support, Adapting to the inherent dynamic nature of WSNs, Sensor Networks and mobile robots.

Text Books:

1. Ad Hoc and Sensor Networks – Theory and Applications, Carlos Corderio Dharma P. Aggarwal, World Scientific Publications, March 2006, ISBN – 981–256–681–3.
2. Wireless Sensor Networks: An Information Processing Approach, Feng Zhao, Leonidas Guibas, Elsevier Science, ISBN – 978-1-55860-914-3 (Morgan Kauffman).

CYBER LAWS AND SECURITY POLICIES
(Program Specific Elective - V)

Objectives

1. To understand the computer security issues
2. To make secure system planning, policies

Outcomes

Students who successfully complete this class will be able to:

1. Describe laws governing cyberspace and analyze the role of Internet Governance in framing policies for Internet security
2. the importance of ethics in legal profession and determine the appropriate ethical and legal behavior according to legal frameworks

UNIT - I

Introduction to Computer Security: Definition, Threats to security, Government requirements, Information Protection and Access Controls, Computer security efforts, Standards, Computer Security mandates and legislation, Privacy considerations, International security activity.

UNIT - II

Secure System Planning and administration, Introduction to the orange book, Security policy requirements, accountability, assurance and documentation requirements, Network Security, The Red book and Government network evaluations.

UNIT - III

Information security policies and procedures: Corporate policies- Tier 1, Tier 2 and Tier3 policies - process management-planning and preparation-developing policies-asset classification policy-developing standards.

UNIT - IV

Information security: fundamentals-Employee responsibilities- information classification- Information handling- Tools of information security- Information processing-secure program administration.

UNIT - V

Organizational and Human Security: Adoption of Information Security Management Standards, Human

Factors in Security- Role of information security professionals.

References

1. Debby Russell and Sr. G.T Gangemi, "Computer Security Basics (Paperback)", 2nd Edition, O' Reilly Media, 2006.
2. Thomas R. Peltier, "Information Security policies and procedures: A Practitioner's Reference", 2nd Edition Prentice Hall, 2004.
3. Kenneth J. Knapp, "Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions", IGI Global, 2009.

4. Thomas R Peltier, Justin Peltier and John blackley, "Information Security Fundamentals", 2nd Edition, Prentice Hall, 1996
5. Jonathan Rosenoer, "Cyber law: the Law of the Internet", Springer-verlag, 1997
6. James Graham, "Cyber Security Essentials" Averbach Publication T & F Group.

INTERNET OF THINGS
(Program Specific Elective - V)

Objectives

1. Students will be explored to the interconnection and integration of the physical world and the cyber space. They are also able to design & develop IOT Devices.

Outcomes

1. Able to understand the application areas of IOT
2. Able to realize the revolution of Internet in Mobile Devices, Cloud & Sensor Networks
3. Able to understand building blocks of Internet of Things and characteristics.

UNIT - I

Introduction to Internet of Things –Definition and Characteristics of IoT, Physical Design of IoT – IoT Protocols, IoT communication models, Iot Communication APIs, IoT enabled Technologies – Wireless Sensor Networks, Cloud Computing, Big data analytics, Communication protocols, Embedded Systems, IoT Levels and Templates, Domain Specific IoTs – Home, City, Environment, Energy, Retail, Logistics, Agriculture, Industry, health and Lifestyle.

UNIT - II

IoT and M2M – Software defined networks, network function virtualization, difference between SDN and NFV for IoT. Basics of IoT System Management with NETCOZF, YANG-NETCONF, YANG, SNMP NETOPEER

UNIT - III

Introduction to Python - Language features of Python, Data types, data structures, Control of flow, functions, modules, packaging, file handling, data/time operations, classes, Exception handling. Python packages - JSON, XML, HTTP Lib, URL Lib, SMTP Lib.

UNIT - IV

IoT Physical Devices and Endpoints - Introduction to Raspberry PI - Interfaces (serial, SPI, I2C). Programming – Python program with Raspberry PI with focus of interfacing external gadgets, controlling output, reading input from pins.

UNIT - V

IoT Physical Servers and Cloud Offerings – Introduction to Cloud Storage models and communication APIs. Webserver – Web server for IoT, Cloud for IoT, Python web application framework. Designing a RESTful web API

TEXT BOOK:

1. Internet of Things - A Hands-on Approach, Arshdeep Bahga and Vijay Madiseti, Universities Press, 2015, ISBN: 9788173719547
2. Getting Started with Raspberry Pi, Matt Richardson & Shawn Wallace, O'Reilly (SPD), 2014, ISBN: 9789350239759