Elective II & Elective III

Credits (3 or 4)

Various Electives Given by the Different Faculty including…

Network Security

Soft Computing

Biometrics

Information Assurance

NETWORK SECURITY

PART I SECURITY CHALLENGES TO COMPUTER NETWORKS

1. SECURITY THREATS TO COMPUTER NETWORKS
   Sources of Security Threats, Security Threat Motives, Security Threat Management, Security Threat Correlation, Security Threat Awareness
2. COMPUTER NETWORK VULNERABILITIES
   Sources of vulnerabilities, Vulnerability Assessment
3. HOSTILE SCRIPTS
   Introduction to the Common Gateway Interface (CGI), CGI Scripts in a Three – Way Handshake, Server – CGI Interface, CGI Script Security Issues, Web Script Security Issues, Dealing with the Script Security Problems, Scripting languages: server side, client side scripting languages

PART II DEALING WITH NETWORK SECURITY CHALLENGES

4. ACCESS CONTROL AND AUTHORIZATION
   Access Rights, Access Control Systems, Authorization, Types of Authorization Systems, Authorization Principles, Authorization Granularity, Web Access and Authorization
5. AUTHENTICATION
   Authentication Elements, Types of Authentication, Authentication Methods, Developing an Authentication Policy
6. FIREWALLS
   Types of Firewalls, Configuration and Implementation of a Firewall, Demilitarized Zone (DMZ), Firewall Services and Limitations
7. SYSTEM INTRUSION DETECTION AND PREVENTION
   Intrusion Detection, Intrusion Detection Systems, Types of Intrusion Detection Systems, Challenges to Intrusion Detection Systems, Intrusion Prevention Systems

PART III WIRELESS NETWORKS

8. SECURITY IN WIRELESS NETWORKS AND DEVICES
   Cellular wireless Communication Network Infrastructure, Wireles LAN (WLAN) or Wireless Fidelity (Wi-Fi), Standards for wireless Networks, Security in Wireless Networks

PART IV PROTOCOLS AND STANDARDS

9. NETWORK SECURITY PROTOCOLS AND STANDARDS
   Application Level Security: PGP, S/MIME, Secure HTTP, HTTPS, Secure Electronic Transactions (SET), Kerboros; Security in the Transport Layer: Secure Socket Layer (SSL), Transport Layer Security (TLS); Security in the Network Layer: Internet Protocol Security (IPSec), Virtual Private Networks (VPNs), Security in the Link Layer and over LANS: Point-to-Point Protocol (PPP), Remote Authentication Dial-In Service (RADIUS), Terminal Access Controller Access Control System (TACACS+)

Soft Computing

Credits: 3

Brief Description of the Course:

Soft Computing methodologies handle imprecision, uncertainty, complexity and partial truth of information arising in real life systems, which include fuzzy logic, rough set, neural networks, and evolutionary computation (EC) as core methodologies. Soft computing methods have proved to be very useful for machine intelligence, automation and technology based Applications demanding high Computational Intelligence. This course covers fundamentals of some important methodologies of Soft computing. It also focuses on their application to Engineering, Economics, Finance and Banking Management. The course deals with Matlab and its relevant toolboxes such as Optimization toolbox, fuzzy logic toolbox, neural network toolbox and control system toolbox along with relevant problems and case studies.

Course Contents:

Module A: Fuzzy Sets and Fuzzy Logic:

Introduction, fuzzy sets versus crisp sets, fuzzy relations, extension principles, fuzzy numbers, linguistic variable, hedges, fuzzy logic, fuzzy rule base design and analysis, fuzzy control system, fuzzy segmentation and clustering, fuzzy decision making.

Module B: Artificial Neural Networks:

Basic models, single and multi layer perceptions, back propagation algorithm for MLP, support vector machine, radial basis function neural networks, general regression neural networks, Probabilistic neural networks, Kohonen's self-organizing feature map, deep learning and deep neural network.

Module C: Evolutionary Techniques:

Basics of genetic algorithm (GA), schema theorem and convergence of GA, differential evolution, ant colony optimization, particle swarm optimization.

Module D: Rough Sets

Definition, upper and lower approximations, boundary region, definability, roughness, reduct and core, decision matrices and applications.

Module E: Hybrid Systems:

Neural network based fuzzy Systems, fuzzy logic based neural networks, genetic Algorithm for neural network design and learning, fuzzy logic and genetic algorithm for optimization.

Text and Reference Books:

1. T. J. Ross, "Fuzzy logic with engineering applications", 3rd Edition, John Wiley & Sons, (2010).
2. H.-J. Zimmermann, "Fuzzy set theory and its applications", 4th edition, Kluwer Academic Publishers, (2001).
3. G. Bojadziev and M. Bojadziev, "Fuzzy sets, fuzzy logic, applications", World Scientific, (1995).
4. G. J. Klir and B. Yuan, "Fuzzy sets and fuzzy logic: theory and applications" Prentice Hall, (1995).
5. S. Haykin, "Neural networks and learning machines" 3rd edition, Prentice Hall, (2008).
6. D. W. Patterson, "Artificial neural networks: theory and applications", Prentice Hall, (1998).
7. M. H. Hassoun, "Fundamentals of artificial neural network", MIT Press, (1995).
8. D. E. Goldberg, "Genetic algorithms in search and optimization, and machine learning", Addison-Wesley, (1989)
9. K. Deb, "Multi-objective optimization using evolutionary algorithms", Wiley India Pvt Ltd, (2010).
10. C.-T. Lin and C. S. G. Lee, "Neural fuzzy systems:a neuro-fuzzy synergism to intelligent systems", Prentice Hall, (1996).
11. Z. Pawlak, "Rough sets: theoretical aspects of reasoning about data", Kluwer Academic Publishers, (1991).

Biometrics

Credits:4

Brief Description of the Course:

Biometrics has emerged as mainstream use for computer authentication, identification document security, and surveillance for public safety. This emergence has been accompanied by an expansion in biometric modality from mainly fingerprints to face, iris, hand, voice, and other novel biometrics. This course concentrates on the unique advantages that biometrics brings to computer security, but also addresses challenging issues such as security strength, recognition rates, and privacy, as well as alternatives of passwords and smart cards.

Course Contents:

Module-A: Biometrics - Physiological or Behavioral, Verification, Identification and Applications, Biometric Technologies, Working of Biometrics, Benefits, Application Design, Performance measures; Fingerprinting: Fingerprint Recognition, Fingerprint Scanning, Practical Applications of Fingerprint Scanning, Accuracy and Integrity, Fingerprint Matching, Fingerprint Classification, Fingerprint Image Enhancement, Fingerprint Feature Extraction, Fingerprint Form Factors, Types of Scanners: Optical - Silicon – Ultrasound, Multispectral Fingerprint Matching.

Module-B: Hand Biometrics: Palm print, Vein pattern, Knuckle, Finger Geometry & Handwriting Recognition: Introduction, Applications, Combining Biometric Methods, Strengths and Weaknesses.

Module-C: Iris & Face Recognition: Introduction, Benefits of Using Iris Technology, Iris-Scan: How it Works, Iris-Scan Applications, Iris-Scan Issues, Introduction to Facial Recognition, How Is Facial Recognition Technology Currently Being Used?, How Well Does Facial Recognition Work, Why Face Recognition, Facial Recognition: How it Works, Image Quality, Facial Scan Process Flow, Verification vs. Identification, Primary Facial Recognition Technologies, Facial Recognition Applications.

Module-D: Voice Recognition & Keystroke Dynamics: Introduction, Working, Strengths and Weaknesses, Voice Recognition Applications, Voice Verification in Telephone Banking, Understanding Voice Recognition, Choice of Features, Speaker Modeling, Pattern Matching, Keystroke Dynamics, Active & Passive Biometrics.

Module-E: Multi-Modal Biometrics: Multi-Modal Biometric Systems, Fusion Methodology, Levels of Fusion, Feature-Extraction Level Fusion, Data Matching Level Fusion, Probabilistic-Decision level Fusion, Fusion Procedure, Modes of Operation, Integration Strategies, Design Issues, Soft Biometrics, A Biometric Vision, Securing Biometric Template: Cancelable biometrics, Authentication, Security Analysis.

Text Books & References:

1. Raud M. Bolle, Jonathan H. Connell, Sharath Panakanti, Nalini K. Ratha, Andrew W. Senior, Guide to biometrics, Springer, 2003.

2. Anil K. Jain, Patrick Flynn, Arun A. Ross, Handbook of Biometrics, Springer, 2007.

3. Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar, Handbook of fingerprint recognition, Springer, 2002.

4. David D. Zhang, Palmprint Authentication, Kluwer Academic Publishers, 2004.

5. Chuck Wilson, Vein pattern recognition- a privacy enhancing biometric, CRC press, 2010.

6. Stan Z. Li, Anil K. Jain, Handbook of face recognition, Springer, 2004.

7. Arun A. Ross, Karthik Nandakumar, Anil K. Jain, Handbook of Multibiometrics, Springer, 2006.

8. Bir Bhanu, Venu Govindaraju, Multibiometrics for human identification, Cambridge University Press, 2011.

9. Hai Zhou Li, Kar Ann Toh, Liyuan Li, Advanced topics in biometrics, World Scientific, 2011.

10. Stan Z. Li, Anil K. Jain, Encyclopedia of Biometrics, Volume 1 & 2. Springer, 2009.

Information Assurance

Credits: 3

Brief Description

IA is considered as a superset of Information security. IA is an Interdisciplinary field in addition to Information Security, it covers accounting, fraud examination, forensic science, management science, systems engineering, security engineering, and criminology, Corporate governance issues. It also focuses privacy, regulatory and standards compliance, auditing, business continuity, and disaster recovery

Course Contents

Module A

- Introduction to Information Assurance, Information Assurance services, Information Security, Cyber Security, Cyber Defense
- Security Engineering - Integrated IA Governance and Metrics
- Forensic science, management science, systems engineering, security engineering, and criminology

Module B

- Analysis of Security events - Prediction, prevention and assurance
- Security Technologies; Host Infrastructure, Application;
- Network Firewalls and Web Application Firewalls

Module C

- Vulnerabilities, hardening, countermeasures and Integrated risk management
- Holistic view of various security components, synergy of threats and counter measures
- IT Laws and Critical Infrastructure protection

Module D

- Case Study and Introduction to Intrusion Detection/ Prevention Systems;
- Case Studies: Compliance in Financial Services;

Module E

Recent Trends & Developments in information assurance

Text books/References

1. Information Assurance, Blyth, Andrew, Kovacich, Gerald L., Springer-Verlag London, 2006

2. Principles of Information Security; Michael E. Whitman &

Herbert J. Mattord; Publisher: Thompson Course Technology, Boston, MA;

3. Information Security: Contemporary Cases; Marie Wright and John Kakalik. Jones and Bartlett, 2007;

4. Wall Street Journal, (Required) Dow Jones, Inc. (In particular look out for the special issues on Telecommunications, Electronic Commerce etc that deal with IT)

6. Managing Information Assurance in Financial Services (eds H. R. Rao, M. Gupta, S. Upadhyaya, Idea Group, 2007)