COMPUTER FORENSICS & CYBER SECURITY

Programme Structure

Course Code	Course Title	Lectures (L) Hours per week	Tutorial (T) Hours per week	Practical (P) Hours per week	Total Credits
FCH2151	Computer Forensics	2	-	2	3
FCH2251	Ethics, Policies and the IT Act	2	1	-	3
FCH2351	Behavioral Biometrics	2	1	-	3
FCH2451	Implementation Practical on MATLAB	-	-	6	3
FCH2551	Cyber Security	2	-	2	3
FCH2651	Incident Response Management	2	1	-	3
	TOTAL				**18**

Syllabus - Semester First

COMPUTER FORENSICS

Course Code: FCH2151 **Credit Units: 3**

Course Objective:

- To correctly define and cite appropriate instances for the application of computer forensics Correctly collect and analyze computer forensic evidence
- Identify the essential and up-to-date concepts, algorithms, protocols, tools, and methodology of Computer Forensics

Course Content:

Module-I: Cyber Crime and computer crime

Introduction to Digital Forensics, Definition and types of cybercrimes, electronic evidence and handling, electronic media, collection, searching and storage of electronic media, introduction to internet crimes, hacking and cracking, credit card and ATM frauds, web technology, cryptography, emerging digital crimes and modules.

Module-II: Basics of Computer

Computer organisation, components of computer- input and output devices, CPU, Memory hierarchy, types of memory, storage devices, system softwares, application softwares, basics of computer languages.

Module-III: Computer Forensics

Definition and Cardinal Rules, Data Acquisition and Authentication Process, Windows Systems-FAT12, FAT16, FAT32 and NTFS, UNIX file Systems, mac file systems, computer artifacts, Internet Artifacts, OS Artifacts and their forensic applications

Module-IV: Forensic Tools and Processing of Electronic Evidence

Introduction to Forensic Tools, Usage of Slack space, tools for Disk Imaging, Data Recovery, Vulnerability Assessment Tools, Encase and FTK tools, Anti Forensics and probable counters, retrieving information, process of computer forensics and digital investigations, processing of digital evidence, digital images, damaged SIM and data recovery, multimedia evidence, retrieving deleted data: desktops, laptops and mobiles, retrieving data from slack space, renamed file, ghosting, compressed files.

Examination Scheme:

Components	CT	HA	S/V/Q	ATTD	EE
Weightage(%)	10	7	8	5	70

CT: Class Test, HA: Home Assignment, S/V/Q: Seminar/Viva/Quiz, ATTD: Attendance EE: End Semester Examination

Text & References:

- C. Altheide& H. Carvey Digital Forensics with Open Source Tools, Syngress, 2011. ISBN: 9781597495868.
- Selected readings from various sources as assigned
- Online Course management System: https://esu.desire2learn.com/

COMPUTER FORENSIC PRACTICAL

List of Exercises

- Live Case Studies
- Open Source Forensic Tools
- Disk Forensics and Data Recovery
- Steganography
- Key loggers
- Network monitors
- Flowchart management
- UML diagrams
- eCommerce on websites

Syllabus - Semester Second

ETHICS, POLICIES AND THE IT ACT

Course Code: FCH2251 **Credit Units: 3**

Course Objective:
To understand the ethics and laws by which cyberspace is governed in our country and worldwide.

Course Contents:
Module-I:
Basics of Law and Technology, Introduction to Indian Laws, Scope and Jurisprudence, Digital Signatures, E Commerce-an Introduction, possible crime scenarios, law coverage, data interchange, mobile communication development, smart card and expert systems

Module-II:
Indian Laws, Information Technology Act 2000, Indian Evidence Act, India Technology Amendment Act 2008, Indian Penal Code , Computer Security Act 1987, National Information Infrastructure Protection Act 1996, Fraud Act 1997, Children Online Protection Act 1998, Computer Fraud and Abuse Act 2001

Module-III:
Intellectual Property, IP Theft, Copyright, Trademark, Privacy and Censorship, Introduction to Cyber Ethics, rights over intellectual property

Module-IV:
Introduction to International Laws, International Cyber Laws, Policy and Compliance, Corporate IT Policy Formulations, Compliance Auditing

Examination Scheme:

Components	CT	HA	S/V/Q	ATTD	EE
Weightage(%)	10	7	8	5	70

CT: Class Test, HA: Home Assignment, S/V/Q: Seminar/Viva/Quiz, ATTD: Attendance EE: End Semester Examination

Text & References:

- CYBER LAW-The Indian Perspective, PawanDuggal (2009)
- 7 Years of Indian Cyber Laws, RohasNagpal (2008)
- Doctrine of IT Act of India, Government of India Publication (2000)

Syllabus - Semester Third

BEHAVIORAL BIOMETRICS

Course Code: FCH2351 **Credit Units: 3**

Course Objective

- To understand techniques used for building speech recognition systems
- To understand the components, issues and approaches for constructing spoken dialogue systems
- To learn the syntax and semantics of speech recognition.
- To have an awareness on the current state-of-the-art in speech recognition
- Know the basic parameters of human gait
- Characterize normal human gait
- Identify type of gait disorder and pathologies
- Know the methods of gait analysis and stability and postural control assessment used in clinical practice

Course Content:

Module-I: BIOMETRICS FUNDAMENTALS
Introduction – Benefits of biometric security – Verification and identification Basic working of biometric matching – Accuracy – False match rate – False non-match rate – Failure to enroll rate – Derived metrics – Layered biometric solutions.

Module-II: SPEECH RECOGNITION
Introduction-Regular Expressions and automata-Words and transducers-N-grams Part of speech tagging-Hidden Markov and Entropy models, Speech-Phonetics-Speech synthesis-Automatic speech recognition-Speech Recognition advanced topics-Computational Phonology

Module-III: SPEECH PARSING&SEMANTICS OF SPEECH RECOGNITION
Formal grammar of English-Syntactic parsing-Statistical parsing-Features and Unification-Language and complexity, Semantics and Pragmatics-The representation of meaning-Computational Semantics-Lexical semantics- Computational lexical semantics-Computational discourse

Module-IV: GAIT PATTERN ANALYSIS
Fundamentals of Gait Analysis , Fundamentals of Gait Analysis, Gait Analysis: Considerations and Terminology , Motion Analysis Systems , Ground Reaction Forces , Introduction to EMG ,Motion Analysis , Normal Gait: Ankle & Foot Complex , Normal Gait: Knee Joint , Normal Gait: Hip Joint ,Normal Gait: Control of the whole body center of mass, Pathological Gait Voice Scan - Features – Components Operation (Steps) – Competing voice Scan (facial) technologies – Strength and weakness.

Examination Scheme:

Components	CT	HA	S/V/Q	ATTD	EE
Weightage(%)	10	7	8	5	70

CT: Class Test, HA: Home Assignment, S/V/Q: Seminar/Viva/Quiz, ATTD: Attendance EE: End Semester Examination

References:

- Daniel Jurafsky and James Martin "Speech and Language Processing", 2nd edition, Prentice- Hall, 2008.
- Xuedong Huang, Alex Acero and Hsiao-Wuen Hon, "Spoken Language Processing", Prentice- Hall, May 2001.
- Paul Taylor,"Text-to-Speech Synthesis", Cambridge University Press, February 2009.
- Samir Nanavati, Michael Thieme, Raj Nanavati "Biometrics – Identity Verification in a Networked World", WILEY- Dream Tech Edition 2009.(UNIT 1,2,3,4,)
- Paul Reid "Biometrics for Network Security", Pearson Education.2009. (UNIT – V)
- John D. Woodward, Jr. Wiley Dreamtech Biometrics- The Ul
- Perry J. Gait analysis. Normal and Pathological Fuction. SLACK Incorporeted, 1992

Syllabus - Semester Fourth

IMPLEMENTATION PRACTICAL ON MATLAB

Course Code: FCH2451 **Credit Units: 3**

List of Exercises

- Speech Sample Collection
- Speech sample Registration
- Speech Sample Analysis: Forensic Freeware
- Biometric Sample Collection: Face, Fingerprint, Iris, Signature
- Biometric Sample Registration
- Motion Analysis: Capture
- Motion Analysis: Examination

Examination Scheme:

Components	TA	LR	V	ATTD	EE
Weightage(%)	10	7	8	5	70

Note: TA-Teacher's Assessment, LR-Lab Record, V-Viva

Text & References:

- Samir Nanavati, Michael Thieme, Raj Nanavati "Biometrics – Identity Verification in a Networked World", WILEY- Dream Tech Edition 2009.(UNIT 1,2,3,4,)
- Paul Reid "Biometrics for Network Security", Pearson Education.2009. (UNIT – V)
- Daniel Jurafsky and James Martin "Speech and Language Processing", 2nd edition, Prentice- Hall, 2008.
- Xuedong Huang, Alex Acero and Hsiao-Wuen Hon, "Spoken Language Processing", Prentice- Hall, May 2001.
- Paul Taylor, "Text-to-Speech Synthesis", Cambridge University Press, February 2009.

Syllabus - Semester Fifth

CYBER SECURITY

Course Code: FCH2551 **Credit Units: 3**

Course Objective:

- Understand the threats in networks and security concepts.
- Apply authentication applications in different networks.
- Understand security services for email.
- Awareness of firewall and it applications.

Course Content:

Module-I:

Ethical hacking, Attack Vectors, Cyberspace and Criminal Behaviour, Clarification of Terms, Traditional Problems associated with Computer Crimes, Realms of Cyber world, brief history of the internet, contaminants and destruction of data, unauthorized access, computer intrusions, white-collar crimes, viruses and malicious code, virus attacks, pornography, software piracy, mail bombs, exploitation, stalking and obscenity in internet, Cyber psychology, Social Engineering.

Module-II:

Introduction to Digital forensics, Forensic software and handling, forensic hardware and handling, analysis and advanced tools, forensic technology and practices, Biometrics: face, iris and fingerprint recognition, Audio-video evidence collection, Preservation and Forensic Analysis.

Module-III:

Investigation Tools, e-discovery, EDRM Models, digital evidence collection and preservation, email investigation, email tracking, IP tracking, email recovery, searc and seizure of computer systems, password cracking

Module-IV:

Forensic Analysis of OS artifact, Internet Artifacts, File System Artifacts, Registry Artifacts, Application Artifacts, Report Writing, Mobile Forensic- identification, collection and preservation of mobile evidences, social media analysis, data retrival, Email analysis from mobile phones.

Examination Scheme:

Components	CT	HA	S/V/Q	ATTD	EE
Weightage(%)	10	7	8	5	70

CT: Class Test, HA: Home Assignment, S/V/Q: Seminar/Viva/Quiz, ATTD: Attendance EE: End Semester Examination

Text & References:

- Charles P. Fleeger, "Security in Computing", Prentice Hall, New Delhi, 2009.
- BehrouzA.Forouzan, ―Cryptography & Network Security‖, Tata McGraw Hill, India, New Delhi, 2009.
- William Stallings, ―Cryptography and Network Security, Prentice Hall, New Delhi, 2006
- Chalie Kaufman, Radia Perlman, Mike Speciner, ―Network Security: Private Communication in a Public Network‖, Pearson Education, New Delhi, 2004.
- Neal Krawetz, ―Introduction to Network Security‖, Thomson Learning, Boston, 2007.
- Bruce Schneier, ―Applied Cryptography‖, John Wiley & Sons, New York, 2004.

CYBER SECURITY PRACTICAL

List of Exercises

- File System Analysis
- Log Analysis
- Network Devices: Modem, Router, Switch, Hub, Repeater
- SQL Injection
- Cross Site Scripting
- Click Jacking
- TCP/IP Attacks
- Botnet analysis
- Malware Analysis
- IR Objectives and Team Building
- Email Tracking
- IP Tracking
- Cyber psychology and Social Engineering Test Profiling

Syllabus - Semester Sixth

INCIDENT RESPONSE MANAGEMENT

Course Code: FCH2651 **Credit Units: 3**

Course Objective:

- Defining an incident relating to cyber security.
- Recognizing an Incident
- Protocols for first on crime scene investigations.
- Government approved handling of computer crime scenarios.

Course Content:

Module-I:
Cyber Incident Statistics, Computer Security Incident, Information as Business Asset, Data Classification, Information Warfare, Key Concepts of Information Security, Vulnerability, Threat and Attacks, Types of Computer Security Incidents, Examples of Incidents, Incidents Categorization, Low Level Incident, Mid Level Incident, High Level Incident

Module-II:
Incident Prioritization, Incident Response, Incident Handling, Disaster Recovery, Technologies and Impacts, Virtualization and Impacts, Estimated Cost of an Incident, Incident Reporting Organizations, Vulnerability Reports, Incident Identification, Need fpr Incidents Response, Goals for Incident Response,

Module-III:
Incident Response and Handling Process; Step 1: Identification; Step 2: Incident Recording; Step 3: Initial Response; Step 4: Communicating the Incident; Step 5: Containment; Step 6: Formulating a Response Strategy; Step 7: Incident Classification; Step 8: Incident Investigation; Step 9: Data Collection; Step 10: Forensic Analysis, Step 11: Evidence Protection; Step 12: Notify External Agencies; Step 13: Eradication; Step 14: System Recovery; Step 15: Incident Documentation; Step 16: Incident Damage and Cause assessment; Step 17: Review and Update the Response Policies

Module-IV:
Incident Response Team development, Security Awareness and Training Checklist, Incident Management, Purpose of Incident management, Incident management process, Incident management team, Incident Response Team and Members, Member Goals and Responsibilities, Developing Skills in Incident Response Personnel, Incident Response Team Structure, Team Dependencies and Services.

Examination Scheme:

Components	CT	HA	S/V/Q	ATTD	EE
Weightage(%)	10	7	8	5	70

CT: Class Test, HA: Home Assignment, S/V/Q: Seminar/Viva/Quiz, ATTD: Attendance EE: End Semester Examination

Text & References:

- CERT-In Guidelines