CENTRAL UNIVERSITY OF KERALA

DEPARTMENT OF COMPUTER SCIENCE

Ph.D (Computer Science)

Programme Structure
(Applicable for 2020 batch onwards)

	CENTRAL UNIVERSITY OF KERALA DEPARTMENT OF COMPUTER SCIENCE Ph.D COMPUTER SCIENCE – PROGRAMME STRUCTURE					
COURSE CODE	**COURSE TITLE**	**CONTACT HRS/WEEK**				**CREDITS**
		LEC	**LAB**	**TUT**	**LIT**	
SEMESTER I						
CSC7101	Research Methodology	2	1	1	0	4
CSC7102	Research and Publication Ethics (RPE)	1	0	1	0	2
CSC71xx	*Course from Basket 1 (Courses related to specific area of research)	2	1	1	0	4
CSC71xx	*Course from Basket 2 (Courses related to specific research proposal)	2	1	1	2	6

***Courses are assigned by the respective Research Advisory Committee (RAC) depending on the research area and research proposal**

LEC – Lecture, LAB – Lab Work, TUT – Tutorial, LIT – Literature Survey

Basket 1 : Courses related to specific area of research	
CSC7111	Pattern Recognition
CSC7112	Cyber Security
Basket 2 : Courses related to specific research proposal	
CSC7121	Sign Language Recognition
CSC7122	Brain Analysis
CSC7123	Audio Visual Speech Recognition and Semantic Summarization
CSC7124	Machine learning approaches for cyber threat detection
CSC7125	DDOS Attacks and Defense Mechanisms
CSC7126	Data Mining Trends and Research Frontiers
CSC7127	Multimodal Signal Processing

Programme Outcomes

The students will be able to attain the following after the completion of Ph.D. Computer Science

(i) Inculcate critical thinking to carry out scientific investigation objectively without being biased with preconceived notions.

(ii) Equip the student with skills to analyze problems, formulate a hypothesis, evaluate and validate results, and draw reasonable conclusions thereof.

(iii) Able to articulate the scientific advances and limitations of results described in the research literature.

(iv) Plan and conduct original research that addresses questions of significance in a particular subject area in Computer Science and related fields.

(v) Prepare students for pursuing postdoc research or careers in industry/academics

(vi) Imbibe effective scientific and/or technical research communication in both oral and writing.

(vii) Continue to acquire relevant knowledge and skills appropriate to professional activities and demonstrate highest standards of ethical issues.

(viii) Create awareness to become an enlightened citizen with commitment to deliver one's responsibilities within the scope of bestowed rights and privileges for supporting the society.

Programme Specific Outcomes

The Computer Science Department's Ph.D program must enable students to attain, by the time of getting awarded with Doctoral degree

(i) An ability to apply knowledge of computing and mathematics appropriately.

(ii) An ability to identify, formulate, and develop solutions to challenges and to analyse, design and develop cost effective solutions to the societal problems.

(iii) An ability to design, implement, and evaluate a computational system to meet desired needs within realistic constraints.

(iv) An understanding of professional, ethical, legal, security, and social issues and responsibilities.

(v) An ability to communicate and engage effectively with diverse stakeholders while designing computational applications.

(vi) An ability to apply mathematical foundations, algorithmic principles, and computer science theory in the modeling and design in a way that demonstrates comprehension of the tradeoffs involved in design choices and to meet realistic constraints.

(vii) identify, analyze, and synthesize scholarly literature relating to the field of research

CSC7101 – Research Methodology

This is a research skill development course.

Course Objective:
The objective of the course is to provide theoretical and practical aspects of formulating viable research questions and to prepare and execute a feasible research

By completing this course, students will obtain the following course/learning outcomes:

1. Knowledge to be gained:
   (i) Identifying the research problem
   (ii) Representation of research problems into computational algorithms
   (iii) Skills in representation data and implementation of mathematical concepts on computers
   (iv) Influence of data representation on numerical algorithms.
2. Skill to be gained:
   (v) Skills in collecting relevant data pertaining to the problem
   (vi) Skills in representation of data and implementation of mathematical concepts using programming languages and research toolboxes
   (vii) Critical analysing the data suitable for developing computational algorithms.
3. Competency to be gained:
   (viii) Computational modelling of data related to the problem
   (ix) writing research papers and research reports

Prerequisites: Nil

Grading:

Lab implementation	– 12%
Paper presentation/writing	– 10%
Assignment/Quiz/presentation	– 8%
Class Test	– 10%
Final Exam	– 60%

Total Contact Hrs. Per Week	4	Assessment –Total	100 Marks
Lectures	2	Continuous Internal Assessment	40 Marks
Lab	1	End Semester Assessment	60 Marks
Tutorial	1	Credits	4

Unit – I
Conducting a literature review, finding/formulating a research question/goal/objective/scope, identification and formation of research problem (Hypothesis), preparing/ conceptualizing research design (experimental or otherwise), research presentations, methods of data collection.

Unit – II
Measures of central tendency and dispersion: mean, median, mode, range, mean deviation and standard deviation. Basic ideas of testing of hypotheses. Tests of significance based on normal, t and Chi-square distributions. Analysis of variance and co-variance.

Unit – III
Writing of research proposal, report and research paper using LaTeX/MS Office with the help of reference management software like Zotero/Mendeley and plagiarism/self-plagiarism detection using iThenticate. Evaluation of research papers. Why, what, when, with whom and where publish?

Unit – IV
Study of any one or more of the common softwares like Matlab, R, Octave, Network simulators, Mathematica etc.

References:
1. R. Panneerselvam, Research Methodology, 2nd Edition, PHL Learning Private Ltd. New Delhi, 2014
2. C.R. Kothari, Research Methodology: Methods and Techniques, 2nd revised edition, New Age International (P) Limited Publishers, New Delhi, 2013

CSC7102 – Research and Publication Ethics (RPE)

This is a skill development course focusing on philosophy of science & ethics, research integrity, publication ethics with hands-on-sessions to identify research misconduct and predatory publications. Indexing/citation databases, open access publications, research metrics (citations, h-index, impact factor, etc.) and plagiarism tools will be introduced in this course.

Course Objective:

The objective of the course is to provide awareness about the publication ethics, publication misconducts, research integrity, indexing, research metrics and plagiarism.

By completing this course, students will obtain the following course/learning outcomes:

1. Knowledge to be gained:
   (i) Philosophy and ethics of research
   (ii) Scientific Conduct
   (iii) Publication ethics and misconduct
   (iv) Databases and research metrics
2. Skill to be gained:
   (v) Skills to identify research misconduct and predatory publications
3. Competency to be gained:
   (vi) To do effectual research by properly following research ethics

Prerequisites: Nil

Grading:

Group Discussion	– 12%
Paper reviewing and analysis	– 15%
Assignment/Quiz/presentation	– 8%
Class Test	– 5%
Final Exam	– 60%

Total Contact Hrs. Per Week	2	Assessment –Total	100 Marks
Lectures	1	Continuous Internal Assessment	40 Marks
Lab	0	End Semester Assessment	60 Marks
Tutorial	1	Credits	2

Theory : Units 1, 2, 3
Practice: Units 4, 5, 6

Unit 1: PHILOSOPHY AND ETHICS (3 hrs.)

Introduction to philosophy: definition, nature and scope, concept, branches. Ethics: definition, moral philosophy, nature of moral judgments and reactions.

Unit 2: SCIENTIFIC CONDUCT (5 hrs.)

Ethics with respect to science and research. Intellectual honesty and research integrity. Scientific misconducts: Falsification, Fabrication, and Plagiarism (FFP). Redundant publications: duplicate and overlapping publications, salami slicing. Selective reporting and misrepresentation of data

Unit 3: PUBLICATION ETHICS (7 hrs.)

Publication ethics: definition, introduction and importance. Best practices / standards setting initiatives and guidelines: COPE, WAME, etc. Conflicts of interest. Publication misconduct: definition, concept, problems that lead to unethical behavior and vice versa, types. Violation of publication ethics, authorship and contributorship. Identification of publication misconduct, complaints and appeals. Predatory publisher and journals

Unit 3: OPEN ACCESS PUBLISHING (4 hrs.)

Open access publications and initiatives. SHERPA / RoMEO online resource to check publisher copyright & self-archiving policies. Software tool to identify predatory publications developed by SPPU. Journal finder / journal suggestion tools viz. JANE, Elsevier Journal Finder, Springer Journal Suggester, etc.

Unit 5: PUBLICATION MISCONDUCT (4 hrs.)

A. Group Discussions (2 hrs.).
   Subject specific ethical issues, FFP, authorship. Conflicts of interest. Complaints and appeals: examples and fraud from India and abroad.
B. Software tools (2 hrs.).
   Use of plagiarism software like Turnitin, Urkund and other open source software tools.

Unit 6: DATABASES AND RESEARCH METRICS (7 hrs.)

A. Databases (4 hrs.).
   Indexing databases. Citation databases: Web of Science, Scopus, etc.
B. Research Metrics (3 hrs.).
   Impact Factor of journal as per Journal Citation Report, SNIP, SJR, IPP, Cite Score. Metrics: h-index, g index, i10 index, altmetrics

References

1. Bird, A. (2006). Philosophy of Science. Routledge
2. MacIntyre, Alasdair (1967) A Short History of Ethics. London
3. P. Chaddah, (2018) Ethics in Competitive Research: Do not get scoped; do not get plagiarized, ISBN: 978-9387480865
4. National Academy of Science, National Academy of Engineering and Institute of Medicine. (2009). On Being a Scientist: A guide to Responsible Conduct in Research: Third Edition, National Academies Press.
5. Resnik, D. B. (2011). What is ethics in research & why is it important. National Institute of Environmental Health Sciences, 1-10. Retrieved from https://www.niehs.gov/research/resources/bioethics/whatis/index.cfm
6. Beall, J. (2012). Predatory publishers are corrupting open access. Nature, 489(7415), 179-179. https://doi.org/10.1038/489179a
7. Indian National Science Academy (INSA), Ethics in Science Education, Research and Governance (2019), ISBN: 978-81-939482-1-7. http://www.insaindia.res.in/pdf/Ethics_Book.pdf

CSC7111 – Pattern Recognition

This is a practical/lab oriented course focusing on pattern recognition.

Course Objective:

To train the students and make them understand the latest trends in pattern recognition

By completing this course, students will obtain the following course/learning outcomes:

1. Knowledge to be gained:
   (i) Understanding the features and properties of patterns
   (ii) Representation of patterns
2. Skill to be gained:
   (iii) Skills to solve problems using pattern recognition algorithms
3. Competency to be gained:
   (iv) Ability to carry out independent research in pattern recognition

Prerequisites: Nil

Grading:

Lab	– 20%
Assignment/Quiz/presentation	– 10%
Class Test 1	– 5%
Class Test 2	– 5%
Final Exam	– 60%

Total Contact Hrs. Per Week	4	Assessment –Total	100 Marks
Lectures	2	Continuous Internal Assessment	40 Marks
Lab	1	End Semester Assessment	60 Marks
Tutorial	1	Credits	4

Module 1

Pattern Recognition Systems –Definitions, data representation, representations of patterns and classes. Types of pattern recognition systems. Applications of pattern recognition systems. Bayesian decision making and Bayes Classifier for continuous and discrete features.

Module 2

Min-max and Neymann-Pearson classifiers, Discriminant functions, decision surfaces. Maximum likelihood estimation and Bayesian parameter estimation. Overview of Nonparametric density estimation –Histogram based approach, classification using Parzen window.

Module 3

K-nearest neighbour estimation and classification. Classification of clustering algorithms –hierarchical clustering –agglomerative clustering. Partitional clustering –Forgy's algorithm. K-means clustering.

Module 4

Introduction to feature selection –filter method –sequential forward and backward selection algorithms. Wrappers method and embedded methods. Feature extraction methods –principal component analysis, fisher linear discriminant analysis, ICA.

References:

1. Duda R.O., Hart P.E., Stork D.G., *Pattern Classification*, John Wiley and Sons, 2nd Edition, 2001
2. Bishop C.M., *Pattern Recognition and Machine Learning*, Springer, 2nd Edition, 2006
3. Theodoridis S., Pikrakis A., Koutroumbas K., Cavouras D., *Introduction to Pattern Recognition: A Matlab approach*, Academic Press, 2010

CSC7112 – Cyber Security

This is a practical/lab oriented course focusing on cyber security.

Course Objective:

To train the students and make them understand the latest trends in cyber security.

By completing this course, students will obtain the following course/learning outcomes:

1. Knowledge to be gained:
   (i) Understanding the possible threats in cyber world
2. Skill to be gained:
   (ii) Skills to avoid possible cyber threats and detect new type of threats.
3. Competency to be gained:
   (iii) Ability to carry out independent research in Cyber Security

Prerequisites: Nil

Grading:

Lab	– 20%
Assignment/Quiz/presentation	– 10%
Class Test 1	– 5%
Class Test 2	– 5%
Final Exam	– 60%

Total Contact Hrs. Per Week	4	Assessment –Total	100 Marks
Lectures	2	Continuous Internal Assessment	40 Marks
Lab	1	End Semester Assessment	60 Marks
Tutorial	1	Credits	4

Unit I

Introduction to Cyber Security, Cyber Security Goals & policies, Domain of Cyber Security Policy, Elements, Cyber Security Evolution, Implementing Hardware Based Security, Software Based Firewalls, Security Standards, assessing threat levels, forming an Incident Response Team, difference between cyber forensics and cyber security

Unit II

Classifications of Cybercrime, E-Mail Spoofing, Spamming, Cyber defamation, Industrial Spying/Industrial Espionage, Hacking, Software Piracy, Password Sniffing, Credit Card Frauds, Cyberstalking, Botnets, Phishing, Pharming, Password Cracking, Keyloggers and Spywares, Virus and Worms, Trojan Horses and Backdoors, DoS and DDoS Attacks, Malware, Ransomware, Types of Identity Theft, Techniques of ID Theft, Cyber terrorism

Unit III

Significance of Buffer Overflow Vulnerability, Why Programs/Applications are vulnerable. Reasons for Buffer Overflow Attacks. Methods of trapping buffer overflows. Active and passive sniffing, Sniffing countermeasures. ARP poisoning and countermeasures. Man in the middle attacks, Spoofing attacks. SQL Injection, Attacking SQL Servers, Brute Forcing and Application Configuration Files, Input validation attacks. Preventive Measures.

Unit IV

Network defense tools, Secure protocols, Firewalls, VPNs, Tor, I2P, Intrusion Detection and filters, Host-Based IDS vs Network-Based IDS, Dealing with unwanted traffic, Malicious Software & Security, Malicious Web, Internet Security Issues, Types of Internet Security Issues, Secure Coding, Electronic & Information Warfare.

Reference Books:

1. William Stallings, Network Security Essentials: Applications and Standards, Prentice Hall, 4th edition, 2010.
2. David Salomon, Foundations of Computer Security, Springer, 2006.
3. Walter Turner, Cyber Security for You, Kindle Edition, Secure Web Apps, 2016
4. Michael T. Goodrich and Roberto Tamassia, Introduction to Computer Security, Addison Wesley, 2011.
5. Anderson, Ross. Security Engineering: A Guide to Building Dependable Distributed Systems. New York: John Wiley & Sons. 2001.
6. J. P. Anderson, “Computer Security Threat Monitoring and Surveillance,” Technical Report, James P. Anderson Company, Fort Washington, 1980.

CSC7121 – Sign Language Recognition

This is a practical/lab oriented course focusing on sign language recognition.

Course Objective:

To train the students and make them understand the methods of recognizing sign languages.

By completing this course, students will obtain the following course/learning outcomes:

1. Knowledge to be gained:
   (i) Understanding the possible deviations/variations in sign languages
2. Skill to be gained:
   (ii) Skills to find effectual features of sign languages.
   (iii) Skills to write algorithms for sign language recognition
3. Competency to be gained:
   (iv) Ability to develop methods for effectual sign language recognition.

Prerequisites: Nil

Grading:

Final Exam – 100%

Total Contact Hrs. Per Week	6	Assessment –Total	100 Marks
Lectures	2	Continuous Internal Assessment	Nil
Lab	1	End Semester Assessment	100 Marks
Tutorial	1	Credits	6
Literature Survey	2		

Module 1

Distance measures. Image enhancement in spatial and frequency domains. Morphological operations.

Module 2

Image Segmentation: Detection of discontinuities:-point detection-line detection-edge detection. Hough transforms. Thresholding:-simple, global and optimal. Region-based segmentation: -Region growing, region splitting/merging. Colourimage segmentation.

Module 3

Image features. Background/foreground estimation. Object detection/classification. Object tracking. Image/Video analysis and understanding.

Module 4

Literature review on (i) object/image features, (ii) segmentation, (iii) object detection, (iv) object tracking, (v) sign language recognition methods, (vi) sign language recognition features, and (vii) sign language recognition databases.

Reference:

1. Rafael C. Gonzalez, *Digital Image Processing*, Pearson Education, 3 edition (2013), ISBN-10: 9332518467, ISBN-13: 978-9332518469
2. Richard Szeliski, *Computer Vision: Algorithms and Applications*, Springer, 2011, ISBN 1868-0941, ISBN 978-1-84882-934-3

CSC7122 – Brain Analysis

This is a practical/lab oriented course focusing on the analysis of Brain.

Course Objective:

To train the students and make them understand the methods of understanding the brain.

By completing this course, students will obtain the following course/learning outcomes:

1. Knowledge to be gained:
   (i) Understanding the possible ways for analysing the brain
2. Skill to be gained:
   (ii) Skills to find effectual features for brain analysis.
   (iii) Skills to write algorithms for brain analysis
3. Competency to be gained:
   (iv) Ability to develop methods for effectual understanding of brain images/signals.

Prerequisites: Nil

Grading:

Final Exam – 100%

Total Contact Hrs. Per Week	6	Assessment –Total	100 Marks
Lectures	2	Continuous Internal Assessment	Nil
Lab	1	End Semester Assessment	100 Marks
Tutorial	1	Credits	6
Literature Survey	2		

Module 1

Distance measures. Image/signal enhancement in spatial and frequency domains. Morphological operations. Signal/image pre-processing.

Module 2

Image Segmentation: Detection of discontinuities: -point detection -line detection -edge detection. Hough transforms. Thresholding: -simple, global and optimal. Region-based segmentation: -Region growing, region splitting/merging. Colour image segmentation.

Module 3

Image/signal features. Image/Signal Registration. Image/signal classification. Modalities like EEG, MRI, CT, etc.

Module 4

Literature review on (i) signal/image features, (ii) image/signal pre-processing, (iii) image/signal –registration, (iv) image/signal –normalization, (v) statistical analysis of brain using EEG/MRI.

Reference:

1. Rafael C. Gonzalez, *Digital Image Processing*, Pearson Education, 3 edition (2013), ISBN-10: 9332518467, ISBN-13: 978-9332518469
2. Richard Szeliski, *Computer Vision: Algorithms and Applications*, Springer, 2011, ISBN 1868-0941, ISBN 978-1-84882-934-3

CSC7123 – Audio Visual Speech Recognition and Semantic Summarization

This is a practical/lab oriented course focusing on the audio visual speech.

Course Objective:

To train the students and make them understand the methods of understanding the audio visual speech.

By completing this course, students will obtain the following course/learning outcomes:

1. Knowledge to be gained:
   (i) Understanding the possible ways for analysing the audio visual speech.
2. Skill to be gained:
   (ii) Skills to find effectual features for audio visual speech.
   (iii) Skills to write algorithms for the analysis of audio visual speech.
3. Competency to be gained:
   (iv) Ability to develop methods for effectual understanding of audio visual speech.

Prerequisites: Nil

Grading:

Final Exam – 100%

Total Contact Hrs. Per Week	6	Assessment –Total	100 Marks
Lectures	2	Continuous Internal Assessment	Nil
Lab	1	End Semester Assessment	100 Marks
Tutorial	1	Credits	6
Literature Survey	2		

Module 1

Basic elements of a Digital Signal Processing Systems, Classification of Signals, The Concept of Frequency in Continuous -Time and Discrete –Time Signals, The Speech Signal: Speech Production Mechanism, perception-Acoustic Phonetic Characterization and classification -The Speech Production Process-Representing speech in Time Frequency Domains-Speech Sounds and Features. Speech Analysis: The Bank of Filters Front End Processor-Linear Predictive Coding for Speech Recognition-Vector Quantization.

Module 2

Audio detection-Time delay estimation, Beamforming, Visual tracking algorithms:-Template matching and Mean-shift algorithms, Multimodal integration -likelihood combination, Tracker output combination, Partitioned sampling.

Module 3

Representing Meaning: Meaning Structure of Language, Predicate-Argument Structure, First Order Predicate Calculus. Semantic Analysis: Syntax-Driven Semantic Analysis, Attachments for a Fragment of English, Lexical Semantics: Relations among Lexemes and Their Senses, WordNet: A Database of Lexical Relations, The internal Structure of Words.

Module 4

Literature review on (i) Speech and audio processing (ii) Audio visual speech processing (iii) Language processing (iv) Semantic analysis and (v) Multimodal speech processing.

References:

1. Fundamentals of Speech Recognition- Lawrence Rabiner, Biing-Hwang Juang, Prentice Hall. 1993
2. Digital processing of speech signals- L.R. Rabiner and R.W Schafer, Prentice Hall, 1978
3. Speech and Language Processing- Daniel Jurafsky and James H. Martin, Prentice Hall, 2000
4. Audio –Visual Person Tracking A Practical Approach – Fotios Talantzis, A.Pnevmatikakis and A.G. Constatinides, Imperial College Press, 2012

CSC7124 – Machine Learning Approaches for Cyber Threat Detection

This is a practical/lab oriented course focusing on the cyber threat detection.

Course Objective:

To train the students and make them understand the methods of detecting cyber threats.

By completing this course, students will obtain the following course/learning outcomes:

1. Knowledge to be gained:
   (i) Understanding the possible ways for analysing the cyber threat.
2. Skill to be gained:
   (ii) Skills to find effectual features of cyber threat.
   (iii) Skills to write algorithms for the analysis of cyber threat.
3. Competency to be gained:
   (iv) Ability to develop methods for effectual detection of cyber threat.

Prerequisites: Nil

Grading:

Final Exam – 100%

Total Contact Hrs. Per Week	6	Assessment –Total	100 Marks
Lectures	2	Continuous Internal Assessment	Nil
Lab	1	End Semester Assessment	100 Marks
Tutorial	1	Credits	6
Literature Survey	2		

Unit I

Review of Cybersecurity Solutions, Reactive Security Solutions, Misuse/Signature Detection, Anomaly Detection, Hybrid Detection, Scan Detection, Profiling Modules, Understanding the Fundamental Problems of Machine-Learning Methods in Cybersecurity, Incremental Learning in Cyberinfrastructures, Feature Selection/Extraction for Data with Evolving Characteristics, Privacy-Preserving Data Mining

Unit II

Supervised Learning for Misuse/Signature Detection: Machine Learning in Misuse/Signature Detection, Machine-Learning Applications in Misuse Detection, Rule-Based Signature Analysis; Machine Learning for Anomaly Detection: Machine Learning in Anomaly Detection Systems, Machine-Learning Applications in Anomaly Detection, Rule-Based Anomaly Detection, Unsupervised Anomaly Detection.

Unit III

Machine Learning in Hybrid Intrusion Detection Systems, Machine-Learning Applications in Hybrid Intrusion Detection, Anomaly–Misuse Sequence Detection System, Association Rules in Audit Data Analysis and Mining, Misuse–Anomaly Sequence Detection System; Emerging Challenges in Cybersecurity: Emerging Cyber Threats, Network Monitoring, Profiling, and Privacy Preservation, Emerging Challenges in Intrusion Detection.

Unit IV

Literature review on (i) Malware Detection and Classification (ii) Botnet Detection (iii) Drive-By Download Attacks (iv) Network Intrusion Detection (v) File Type Identification (vi) Network Traffic Identification (vii) SPAM Identification (viii) Insider Threat Detection

Reference Books:

1. Ankit Fadia, Manu Zacharia, Network intrusion alert: an ethical hacking guide to intrusion detection, Thomson Course Technology PTR, 2007.
2. Roberto Di Pietro, Luigi V. Mancini, Intrusion Detection System, Springer ,2008.
3. Sumeet Dua, Xian Du, Data Mining and Machine Learning in Cybersecurity Data Mining and Machine Learning in Cybersecurity, CRC Press, 2011, ISBN -13: 978-1-4398-3943-0 (Ebook).

4. Padmavathi Ganapathi, Shanmugapriya, Handbook of Research on Machine and Deep Learning Applications for Cyber Security, IGI Global, 2019, ISBN13: 9781522596110.
5. Sinan Ozdemir, Soma Halder, Hands-On Machine Learning for Cybersecurity, Packt Publishing, 2018.
6. Daniel S. Berman, Anna L. Buczak, Jeffrey S. Chavis and Cherita L. Corbett, A Survey of Deep Learning Methods for Cyber Security, Information, MDPI, 2019.

CSC7125 – DDoS Attacks and Defense Mechanisms

This is a practical/lab oriented course focusing on the DDoS attacks, Cyber Security and Intrusion Detection Systems.

Course Objective:

To train the students and make them understand the defense mechanisms for DDoS attacks.

By completing this course, students will obtain the following course/learning outcomes:

1. Knowledge to be gained:
   (i) Understanding the possible ways for analysing the DDoS attacks.
2. Skill to be gained:
   (ii) Skills to find effectual features of DDoS attacks.
   (iii) Skills to write algorithms for the analysis of DDoS attacks.
3. Competency to be gained:
   (iv) Ability to develop methods for effectually defending DDoS attacks.

Prerequisites: Nil

Grading:

Final Exam – 100%

Total Contact Hrs. Per Week	6	Assessment –Total	100 Marks
Lectures	2	Continuous Internal Assessment	Nil
Lab	1	End Semester Assessment	100 Marks
Tutorial	1	Credits	6
Literature Survey	2		

Unit I

DDoS Attacks: Overview, Criminals, Thrill Seekers and Status Seekers, Hacktivist, Common Types of DDoS Attacks, Volumetric Floods, Network Protocol–Level Attacks, Amplification and Reflection, Application-Level Attacks, Multivector Attacks, Botnets and IoT Devices.

Unit II

DDoS Detection, types of DDoS Detection, DDoS Mitigation and Countermeasures, DDoS Mitigation Topology, Mitigation Tools & Devices, Evaluating Cloud-Based Mitigation Vendors, Cloud-Based DDoS Mitigation Methods, DDoS Event Reporting, Hybrid Model.

Unit III

DDoS Focused Threat Intelligence, IP Blocklists, Community Supported Efforts, IP Geolocation Providers, Purpose-Built Node Lists, Honeypots, DDoS-as-a-Service, DDoS Detection Mechanism in the Cloud, DDoS Mitigation Mechanism in the Cloud.

Unit IV

Literature review on (i) DDoS attacks and detection in Software Defined Networks (ii) DDoS attacks and detection in Cloud Computing (iii) Mitigating DDoS attacks in SDN (iv) Mitigating DDoS attacks in Cloud Computing

Reference Books:

1. Distributed Denial of Service (DDoS), by Rich Groves, Eric Chou, Publisher: O'Reilly Media, Inc., Release Date: April 2018, ISBN: 9781492026181
2. DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance, Dhruba Kumar Bhattacharyya, Jugal Kumar Kalita, Publisher: Chapman and Hall/CRC; 1 edition, 2016, ISBN-10: 1498729649
3. An Introduction to DDoS Attacks and Defense Mechanisms: An Analyst's Handbook, by B. B. Gupta, Publisher: LAP LAMBERT Academic Publishing, 2011, ISBN-10: 3846595691, ISBN-13: 978-3846595695

4. Detection and Defeating Distributed Denial of Service (DDoS) Attacks, Seyed Mohammad Reza Khalifeh Soltanian, Iraj Sadegh Amiri, CreateSpace Independent Publishing Platform, 2014, ISBN-10: 1500568872, ISBN-13: 978-1500568870
5. DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance, Dhruba Kumar Bhattacharyya, Jugal Kumar Kalita, Chapman & Hall/CRC ©2016, ISBN:1498729649, 9781498729642
6. S. Dong, K. Abbas, and R. Jain, A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments, published in IEEE Access, Volume 7, pp. 80813-80828, 201

CSC7126 – Data Mining Trends and Research Frontiers

This is a practical/lab oriented course focusing on the data mining trends and related technologies.

Course Objective:
The objective of the course is to provide theoretical and practical aspects of complex data mining and design for decision support systems.

By completing this course, students will obtain the following course/learning outcomes:
1. Knowledge to be gained:
   (i) State-of-art pre and post data processing techniques and algorithms for complex data.
2. Skill to be gained:
   (ii) Extract knowledge using advanced data mining techniques form complex data
   (iii) Adapt to new data mining tools
   (iv) Ability to analyse the real world complex data mining problems
3. Competency to be gained:
   (v) Development of data mining algorithms for complex real world problems.
   (vi) Ability to participate in data challenges and to do higher order research.

Prerequisites: Nil

Grading:
Final Exam – 100%

Total Contact Hrs. Per Week	6	Assessment –Total	100 Marks
Lectures	2	Continuous Internal Assessment	Nil
Lab	1	End Semester Assessment	100 Marks
Tutorial	1	Credits	6
Literature Survey	2		

Unit-I
Mining Stream, Time Series, Sequence Data: Mining Data Streams: Methodologies for Stream Data Processing and Stream Data Systems, Stream OLAP and Stream Data Cubes, Frequent-Pattern Mining in Data Streams, Classification of Dynamic Data Streams, Clustering Evolving Data Streams. Mining Time Series Data: Trend analysis, Similarity Search in Time-Series Analysis. Mining Sequences: Sequential Pattern mining, Scalable methods, Periodicity Analysis for Time-Related Sequence Data, Mining Sequence Patterns in Biological Data, Alignment of Biological Sequences.

Unit-II
Graph Mining, Social Network Analysis, and Multirelational Data Mining- Graph Mining-Methods for Mining Frequent Subgraphs, Mining Variant and Constrained Substructure Patterns, Applications, Social Networks, Characteristics of Social Networks, Link Mining- Tasks and Challenges, Mining on Social Networks. Multi-relational Data Mining: ILP Approach to Multirelational Classification, Tuple ID Propagation, Multirelational Classification Using Tuple ID Propagation, Multirelational Clustering with User Guidance.

Unit-III
Mining Spatial, Multimedia, Text, and Web Data:. Spatial Data Mining: Spatial Data Cube Construction and Spatial OLAP, Mining Spatial Association and Co-Location Patterns, Spatial clustering, Classification and trend analysis. Multimedia Data Mining: Similarity Search in Multimedia Data, Multidimensional Analysis of Multimedia Data, Classification and Prediction Analysis of Multimedia Data, Mining Associations in Multimedia Data, Audio and Video Data Mining. Text Mining: - Text Data Analysis and Information Retrieval, Dimensionality Reduction for Text, Text Mining Approaches. Mining the Web Wide Web: Mining the Web Page Layout Structure,

Mining the Web's Link Structures to Identify Authoritative Web Pages. Mining Multimedia Data on the Web, Automatic Classification of Web Documents, Web Usage Mining.

Unit-IV

Applications and Trends in Data Mining: Data Mining Applications, Data Mining for Financial Data Analysis, Data Mining for the Retail Industry, Data Mining for the Telecommunication Industry, Data Mining for Biological Data Analysis, Data Mining in Other Scientific Applications, Data Mining for Intrusion Detection, Data Mining System Products and Research Prototypes, How to Choose a Data Mining System, Examples of Commercial Data Mining Systems, Additional Themes on Data Mining, Theoretical Foundations of Data Mining, Statistical Data Mining, Visual and Audio Data Mining, Data Mining and Collaborative Filtering, Social Impacts of Data Mining, Data Mining, Privacy, and Data Security, Trends in Data Mining.

Unit – V

Literature review on data mining, its applications, latest trends and algorithms

Reference:

1. Jiawei Han, Micheline Kamber, Jian Pei, *Data Mining: Concepts and Techniques*, Morgan Kaufmann, 2nd Ed., 2005.
2. Arun K Pujari, *Data Mining Techniques*, Univerities Press, 2nd Ed., 2010.
3. Da Ruan, Guoqing Chen, Etienne E. Kerre, Geert Wets, *Intelligent Data Mining: Techniques and Applications (Studies in Computational Intelligence)*, Springer, 1st Ed., 2010.
4. MasoudMohammadian, I*ntelligent Agents for Data Mining and Information Retrieval*, Idea Group Publishing, 2004.

CSC7127 – Multimodal Signal Processing

This is a practical/lab oriented course focusing on the data mining trends and related technologies.

Course Objective:
The objective of the course is to equip the students with strong basics in signal processing.

By completing this course, students will obtain the following course/learning outcomes:
1. Knowledge to be gained:
   (i) Develop methods for signal transformation
2. Skill to be gained:
   (ii) Practical Skills in representation of digital signal processing concepts using AI related toolbox/packages.
3. Competency to be gained:
   (iii) Computational modelling of digital signal processing in any real world problems

Prerequisites: Nil

Grading:
Final Exam – 100%

Total Contact Hrs. Per Week	6	Assessment –Total	100 Marks
Lectures	2	Continuous Internal Assessment	Nil
Lab	1	End Semester Assessment	100 Marks
Tutorial	1	Credits	6
Literature Survey	2		

Module 1
Basic elements of a Digital Signal Processing Systems, Classification of Signals, Sampling, reconstruction. Time Domain Representation of Signals and Systems- Discrete Time Signals, Operations on sequences, Discrete time Systems, Linear Time Invariant Discrete Time Systems, Frequency Analysis of Signals- Frequency Analysis of Continuous/Discrete Time Signals, Frequency/Time Domain Signal Properties

Module II
The Speech Signal: Speech Production Mechanism, perception- Acoustic Phonetic Characterization and classification - The Speech Production Process- Representing speech in Time Frequency Domains- Speech Sounds and Features. Speech Analysis: The Bank of Filters Front End Processor- Linear Predictive Coding for Speech Recognition-Vector Quantization.

Module III
Digital Image Fundamentals: - Image representation and modelling - sampling and quantization, Relationships between pixels, Image Enhancement in the spatial domain: - point operations, spatial operations. Color models and conversions, Enhancement in frequency domain, Morphological Image Processing, Image Segmentation

Module IV
Introduction to video processing: Principles of color video processing, Composite versus component video, sampling of video signals, 2D/3D motion estimation: Spectral analysis of video signal: Fourier, CT and Wavelet analysis, Audio visual integration: audio-visual speech processing, audio-Visual emotion/gesture recognition

Module V
Literature review on multimodel signal processing, its applications, latest trends, features and algorithms

References:

1. J.G. Proakis, D.G. Manolakis, Digital Signal Processing – Principles, Algorithms and Appl., Pearson, 2013.
2. Lawerence Rabiner, B.-H. Juang & B Yegnanarayana, “Fundamental od Speech Recognition”, Person, 2009
3. Anil K. Jain, “Fundamentals of Digital Image Processing”, Prentice Hall, US Ed., 1988.
4. William K. Pratt, “Digital Image Processing: PIKS Scientific Inside”, Wiley Interscience, 4th Ed., 2007.
5. G. Bailly, P. Perrier & V.-B. Eric, “Audio Visual Speech Processing”, Cambridge University Press, 2012.
6. Peter E Hart, Richard O Duda & David G Stork, “Pattern Classification”, John Wiley and Sons, 2005.