COURSE CURRICULUM
M.TECH. CYBER SECURITY & M.TECH. IN CSE (AI)

Batch 2024-2026

BOS MEETING DATE: JUNE 29, 2024

DEFENCE INSTITUTE OF ADVANCED TECHNOLOGY

Girinagar, Pune 411025

Defence Institute of Advanced Technology

Girinagar, Pune 411025

School of Computer Engineering and Mathematical Sciences (SoCE&MS)

ABOUT SoCE&MS

In the vibrant landscape of technological digital advancement, the **School of Computer Engineering and Mathematical Sciences** (SoCE&MS) emerged in 2022 as a beacon of innovation and progress. Born with the fusion of the **Department of Computer Science and Engineering (CSE),** the **Department of Applied Mathematics (AM)** and **Data Centre**, the mission is to pioneer breakthroughs in the realm of Computing and Mathematical Sciences. The CSE, our trailblazing department was founded in 1987, with the first MTech course offered in 2009; while AM has been integral part of our institute's history since its inception. We stand on the shoulders of this rich legacy as to strengthen and apply modern digitization, as a step into a future defined by innovation, critical thinking, and scientific excellence.

As SoCE&MS, we offer a tapestry of **FIVE Post-Graduation academic programs** and research ventures, a testament to our commitment to diversity and multidisciplinary. From M.Tech., MS by Research, M.Sc., to Ph.D programs are tailored for scientists of R&D organizations, officers of Tri-Services, GATE-Qualified candidates, & self-financed scholars, our offerings are diverse as the ever-evolving world of technology. Among our flagship **M.Tech. programs** are **Modelling & Simulations, CSE (Artificial Intelligence), Data Sciences,** and **Cyber Security.** The school has extended its arms to science graduates with the introduction of **M.Sc. in Data Science** in 2023.

Our dynamic community comprises approximately 160 post-graduate students per year; fueled by the boundless curiosity of successful 21 Ph.D. completions. They thrive an ecosystem that fosters creativity and explorations, where the cutting-edge laboratories, state-of-art equipment, and a stellar faculty beacon them into the world of tomorrow's technological needs. Our 13 faculty members luminaries in fields ranging from Cyber Security, Artificial Intelligence, and Data Sciences to Ethical hacking, Cryptography, Computational Fluid Dynamics, Image Processing, and the rigorous mathematics.

Research at SoCE&MS isn't just a buzzword; it's our heartbeat. We are on the forefronts of cutting-edge research, impart trainings, actively managing funded projects and ahead in revenue generations. The school has received accolades for recognitions via patents & publications; in various national level hackathons; national & international conferences & seminars, Sports & Cultural events. SoCE&MS is the driving force behind the Data Centre activities, facilitating internet access, email service, and web hosting for DIAT.

SoCE&MS's dedication extends beyond the walls of DIAT. We are championing ATMA- NIRBHAR BHARAT INDIA@75 with PAN-INDIA Certification Courses in Artificial Intelligence & Cyber Security. The customized programs for Tri-Services and other national organizations underscore our commitment to empowerment and growth to build self-reliant nation. With resounding emphasis on research, interdisciplinary collaborations, and a global outlook, SoCE&MS stands tall as the vanguard of education, charting the course for a brighter future, to build self-reliant and sustainable nation. The aspiring candidates are welcome to the SoCE&MS where innovation know no bounds!

Institute Vision

To be a Center of Excellence of international repute for Education, Training and research in Advanced Technologies with a view to strengthen national security and self-reliance.

Institute Mission

To evolve as an Innovative Unique Research University to develop indigenous contemporary Defence related technologies in Navigation Systems, Wireless Sensors, Efficient Propulsion Systems, and Weapon Systems for DRDO and Defence Services, provide technological solutions to the Services optimize combat battlefield effectiveness and above all produce qualified quality manpower which can truly become an instrument for building a strong indigenous technology base in the context of creating a performing Defence Industrial Base in India.

School Vision

To be a Center of Excellence of International repute to provide high-quality education, research, and training in the area of Modelling & Simulation (M&S), Data Science (DS), Cyber Security (CS) and Artificial Intelligence (AI) to promote innovation and entrepreneurship skills among the students with a view to strengthen national security and self-reliance.

School Mission

M1 To build strong education, teaching and research environment in the field of Modelling & Simulation (M&S), Data Science (DS), Cyber Security (CS) and Artificial Intelligence (AI) to meet requirements from Defence, specially related to national security.

M2 To strive for continuous learning, innovation, entrepreneurship and quality research culture amongst the student community through effective government, industry & academia collaboration.

M3 To encourage ethics, team work and technological leadership skills among students to solve complex engineering problems collaboratively by imparting strong theoretical foundation complemented with extensive practical training.

M4 Engage with industry, government, DRDO, Tri-services and PSUs to transfer knowledge

M.Tech in Cyber Security

Introduction: Communication networks and information systems have become an essential factor in economic, social development and almost in every facet of our daily lives. Information systems are vulnerable to one or more types of cyber-attacks. The security of communication networks and information systems and their availability in particular, is therefore of increasing concern. In general, cyber security threats are increasing rapidly, the incidents range from defaced websites to theft of large volumes of intellectual property and money, to even Internet crimes. Cyber security is now a prominent field of study. Professionals who are trained in this field are highly regarded and contribute to strengthening the social, political and financial fabric of modern society.

The domain of cyber security refers to the collection of tools, policies, security concepts, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, organization and user's assets. To survive in an Information Centric Warfare scenario, the tools and techniques of cyber security will provide mechanisms to safeguard the critical systems against related threats & attacks.

Eligibility: Full-time B.E./B.Tech. in Computer Science/ Electronics/ Electrical/ Electronics & Communications/ Telecommunications/ Information Technology/ Cyber Security or equivalent discipline or Full-time M.Sc. in Computer Science/ Mathematics or equivalent discipline with a valid GATE score in- CS, DA, EC, EE, MA, ST, BM, IN. [Computer Science & Information Technology (CS), Data Science & Artificial Intelligence (DA), Electronics & Communication Engineering (EC), Electrical Engineering (EE), Mathematics (MA), Statistics (ST), Biomedical Engineering (BM), Instrumentation Engineering(IN).]

Organization: The program curriculum has been designed considering the Cyber Security requirements of Industry and Defence Research and Development. It is designed and reviewed by a panel of experts from Academia, DRDO labs, IDS, R&D Industry, and Alumni. The course work includes Core and Elective courses related to the Cyber Security domain.

Each subject of 4 credits is delivered by subject experts over the duration of 16 weeks approximately. It consists of 3 hrs. of classroom interaction and 2 hrs. of lab sessions per week. The evaluations follow a continuous assessment process that includes – 3 monthly evaluation exams (10 Marks each), an internal assessment (20 Marks), and a final examination (50 Marks). The lab focuses on practical exposure to the Cyber Security tools and techniques in the form of mini-projects and lab assignments. The 3rd and 4th semesters have a major component of M.Tech. project dissertation, where the students work under close supervision and guidance of their project guide. The students present their work at the end of 3rd and 4th semester. The M.Tech. thesis is submitted and evaluated by the panel of expert examiners at the end of the 4th semester.

Program Educational Objectives (PEOs)

PEO1 The M.Tech. courses of SoCE&MS aim at developing skilled Human Resources in the field of Digitization by providing different specializations in M&S, DS, CS, and AI; catering to the emerging multidisciplinary problem-solving needs of defense, civil, and DRDO sectors.

PEO2 M.Tech. in Cyber Security (CS) programme aims at developing skilled Human Resources in the field of Cyber Security with a thrust on solving defence and society-related problems. The present program is conceived to understand, assimilate & use advanced technologies such as Network security, Cryptography, Ethical Hacking, Digital Forensic, Malware Analysis, Information Security Management and Trusted Computing techniques. After completing this course, students are expected to understand and practice the essential CS concepts along with developing secure systems.

PEO3 M.Tech. Computer Science and Engineering with specialization in Artificial Intelligence programme aims at developing skilled Human Resources in the field of AI with a thrust on solving defence and society related problems. The present programme is conceived to understand, assimilate & apply the advanced technologies such as deep learning, robotics, machine learning, computer vision, video surveillance, text analytics, speech analytics etc. After completing this course, students are expected to understand and practice the essential AI concepts along with developing AI based systems to solve society/defence related problems, carry out research and innovation.

Program Outcomes (PO)

PO1 The M.Tech. in Cyber Security & M.Tech in CSE with specialization in AI aim at developing an ability in students to independently carry out research /investigation and development work to solve practical problems.

PO2 The M.Tech. Cyber Security & Computer Science and Engineering aim at developing an ability in students to write and present a substantial technical report/document.

PO3 The M.Tech. students should be able to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program.

Program Specific Outcomes (PSO)

PSO1 The M.Tech. Computer Science and Engineering aims at developing skilled knowledgeable Human task force in the field of Cyber Security, catering the needs of defence, social and DRDO requirements

PSO2 The M.Tech. Computer Science and Engineering aims at developing skilled knowledgeable Human task force in the field of Artificial Intelligence, catering the needs of defence, social and DRDO requirements.

SEMESTER I

Sl. No.	Course Code	Course	Contact Hours/week		Credits
			L	T/P	
1	CS-601	Data Security & Privacy	3	1	4
2	CS-602	Machine Learning for Cyber Security	3	1	4
3	CS-603	Applied Cryptography	3	1	4
4	CS-604	Advanced System Security	3	1	4
5	CS-605	Network and Cloud Security	3	1	4
6	AM-607	Mathematics for Engineers	3	1	4
7	PGC-601	Research Methodology and IPR	2	0	2
		Total	**20**	**6**	**26**

SEMESTER II

Sl. No.	Course Code	Course	Contact Hours/week		Credits
			L	T/P	
1	CS-611	Digital Forensics	3	1	4
2	CS-612	Reverse Engineering & Malware Analysis	3	1	4
3		Elective – I (From Department)	3	1	4
4		Elective – II (From Department)	3	1	4
5		Elective – III	3	1	4
6		Elective – IV	3	1	4
7	PGC-602	Audit 1 and 2	2	0	2
		Total	**20**	**6**	**26**

SEMESTER III

Sl. No.	Course Code	Course	Contact Hours /week		Credits
			L	T/P	
1	CS-651	M.Tech. Dissertation Phase-I	28		14
		Total	**28**		**14**

SEMESTER IV

Sl. No.	Course Code	Course	Contact Hours /week		Credits
			L	T/P	
1	CS-652	M.Tech. Dissertation Phase-II	28		14
		Total	**28**		**14**

List of Subjects (Applicable for Sem - II):

Sr.No.	Course Code	Course
1.	**PGC-602**	English for Research Paper Writing
2.		Disaster Management
3.		Sanskrit for Technical Knowledge
4.		Value Education
5.		Constitution of India
6.		Pedagogy Studies
7.		Stress Management by Yoga
8.		Personality Development through Life Enlightenment Skills

List of Electives/Open Electives (Applicable for Sem - II):

Sr.No.	Course Code	Course
1.	CS-613	Security Standards & Penetration Testing
2.	CE 695A	Cyber Physical Systems
3.	CE 70G	Blockchain Technology
4.	CE 66A	Algorithmic Cryptanalysis
5.	CE606A	Software Engineering & System Modelling
6.	CE699	Internet of Things
7.	CE 681	Mobile Computing
8.	CE 683	Information Warfare
9.	CE 689	Fault Tolerant Computing Systems

10.	CE 690	Parallel & Distributed Systems
11.	CE 688	Game Theory
12.	CE 667	Trustworthy Computing
13.	CE 692	Computational Geometry & Applications
14.	CE 698	Multimedia Security
15.	CE 695	Cyber-Physical & Self-Organizing Systems
16.	CE 69B	Network Forensics
17.	CE 602A	Computational Intelligence
18.	CE 70A	Formal Specification and Verification of Programs
19.	CE 70B	Advanced Algorithms
20.	CE 700	Quantum Computing
21.	CE 70D	Computer Network Audit & Forensics
22.	CE 697	Biometric Security
23.	CE 70E	Machine Learning in Python
24.	CE 70F	Cloud Computing
25.	CE 70H	Cyber Security and Cryptography for Embedded Systems
26.	CE 682	Secure Software Engineering
27.	CE 69F	Theory of Computation
28.	CE 691	Secure Wireless Sensor Networks
29.	*AM 625*	*Digital Image Processing*
30.	*AM 628*	*Computational Number Theory and Cryptography*
31.	*EE 613*	*Electronic Warfare*
32.	*TM 609*	*System Engineering*
33.	*MOOC*	*Any relevant MOOC course for 4 credits upon*

SubjectCode	CS-601
Subject title	**Data Security & Privacy**
Credit	**04**
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	1. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 2. One Final Evaluation at the End of the Term **50 Marks** 3. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	None. First 10 hours will be devoted for Prerequisite learnings related to basics of Databases (04 hours), Computer Networks (02 Hours), Operating System (02 Hours),Trends in evolutions of Compute-Devices (02 Hours)
About theCourse	I. As data collection and information networks expand (and stories of security breaches and the misuse of personal information abound), data security and privacy issues are increasingly central parts of the information policy landscape. II. Legislators, regulators, businesses, and other institutions of all kinds are under increasing pressure to draft and implement effective laws, regulations, and security and privacy programs under rapidly changing technological, business, and legal conditions. III. A strong need is arising for individuals with the training and skills to work in thisunsettled and evolving environment. IV. This course will examine: 1) security issues related to the safeguarding of sensitive personal and corporate information against inadvertent disclosure; 2) policy and societal questions concerning the value of security and privacy regulations, the real world effects of data breaches on individuals and businesses, and the balancing of interests among individuals, government, and enterprises; 3) current and proposed laws and regulations that govern information security and privacy; 4) private sector regulatory efforts and self- help & system design measures; 5) emerging technologies that may affect security and privacy concerns; and 6) issues related to the development of enterprise data security programs, policies, and procedures that take into account the requirements of all relevant constituencies; e.g., technical, business, and legal. V. This course is intended for students and professionals in information policy, public policy, business, and information science who have an interest in work or research in security and privacy fields, or in support of those fields. VI. Along with traditional responsibilities individuals may have new security considerations, e.g., programming. The course will include individual reading and writing assignments, class discussion, case studies, and a group assignment. Students will have some latitude to tailor the assignments to theirskills and interests.
Course Objectives	• The growth of importance of information security and privacy matters in the government and enterprise arenas has significantly broadened the scope of individuals who must be aware of relevant issues as part of their work. Securityis becoming more of an element of existing roles such as records management, and new security roles such as Chief Information SecurityOfficer are appearing in the enterprise.

	• Security considerations may become new elements of traditional responsibilities (e.g., programmers historically have been expected to document code, but now should be aware that failure to document may be a factor in a law enforcement investigation of whether a data breach wasforeseeable). • This course will help students to examine policy, and enterprise issues and problems related to security and privacy. • Electronic data will be the focus. Discussions will take general approaches andalso focus on specific technologies.
Course Outcomes	**Bloom's Taxonomy:** **Level-1 Remember; Level-2 Understand; Level-3 Apply; Level-4 Analyze Level-5 Evaluate; Level-6 Create**

CO Title			**Level**	**Descriptor**
	CO1:	Student will be able to examine and identify Data Models for various applications + A general background in concepts of privacy at National & International Scenarios	L1, L2	Remember, Learn
	CO2:	Student will be able to apply data abstraction & normalization techniques to handle volume and veracity + An understanding of how automation is changing the concepts and expectations concerning privacy and the increasingly interconnected issue of security;	L3, L4	Apply, Analyse
	CO3:	Student will be able to analyze & apply multi-dimensional data models for complex scenarios + Knowledge of technologies and regulations concerning information security from both data protection and lawenforcement perspectives.	L4, L5	Analyse, Evaluate
		CO4: Student will be able to propose solutions using various data models to cater special application requirements & to form a base to apply Data Mining & AIML techniques. + Use Case Study and apply Knowledge of the role of private regulatory and self-helpefforts.	L5, L6	Evaluate, Create

Summary of the Course Outcome	At the end of the course, a student will have an understanding of the concepts of datamodels, inherent security mechanisms using data models and issues necessary to address emerging areas of data security and privacy in their potential or current careers. Broadly defined roles include, but certainly are not limited to, systems managers, developers, and engineers; librarians, records managers and other archivists; business managers whose areas of responsibility include systems; data analysts; public and private sector policy professionals; and privacy and securityprofessionals.

Syllabus Details

Basics & Preliminaries	Types of Data Models, Role of Basic and AdvancedData Structures in Data Models, Basic Dictionary Data Types; Algorithms and basics of analysis, OS & Algorithms in Parallel Environments; Protocols of Computer Networks preliminaries,Concerns for Data Security and Privacy	Cormen et al, Horowitz Sahani, Bipin Desai, Korth et al. Kurose Ross	10 Hours	CO1
Unit-1	Security Architectures Information Systems; Database management Systems; Information Security CIA; Information Security Architecture; Database Security levels' Menances to Databases; Asset Types & their values	Text Book-1,Ch-1 Text Book-2, Ch-1	08 Hours	CO1

Unit-2	Database Security Methods Environments: Parallel DBs, Distributed DBs, Database security Methodology; Database Security Definition	Text Book-1,Ch-1 Text Book-2,Ch-2,3	04 Hours	CO1
Unit-3	Profiles, Password Policies, Privileges, and Roles Defining and using Profiles: Creating Profiles in SQLServers & end-users; Password Policies, Privileges, Tables and DatabaseObjects Privileges, Column-Level Privileges; Creating, Assigning, and Revoking User Roles	Text Book-1,Ch-4 Text Book--2, Ch-4	06 Hours	CO1 CO2
Unit-4	Database Application Security Models: Security Models: Access Matrix Model, Access Modes Models; Application Types: Client/Server Application; Web Application, Data Warehouse, Data Stream Applications	Text Book-1,Ch-5 Text Book-2 Ch-5,6,7,8	06 Hours	CO3
Unit-5	Virtual Private Databases: VPD, Implementation, VPD Row Col Security	Text Book-1,Ch 6	06 Hours	CO3
Unit-6	Database Auditing Models Technical Audit Environment, Process, Objectives, Classification Types, Incidence Reports, Level of escalations. Application Data Audit: DML Action Audit; Triggers; Fine-Grained Auditing FGA; Application Errors; PL-SQL Environments, Audit DB Activities	Text Book-1Ch 7, 8, 9 Text Book-2,Ch-12,13	06 Hours	C04
Unit-7	Evolving Models & Security: Big Data; Data Streams; Structured, Unstructured, SQL and NOSQL, BlockChains, NFTs; Database Trojans, SQL Attachments in e-mails; Anatomy of vulnerability SELECT Encrypt data-at-rest & data-at-transit, Dataand AIML Models. Project Cases data Security and Privacy: OnlineDatabases; CSV files to Structured Environments, SCADA, IoTs,	Text Book-1,Ch-10 Text Book-2 Ch.9,10,11	06 Hours	CO1, CO4
Text Books (MUST Know)	Text Book 1 Hassan A. Afyouni,—Database Security and Auditing, Third Edition, CengageLearning,2009. Text Book-2: Ron Ben Natan, Implementing Database Security and Auditing,Elsevier Digital Press, 2005			
Reference Books (SHOULD Know)	Reference Book-1 Charu C. Aggarwal, Philip S Yu —Privacy Preserving Data Mining ‖:Models and Algorithms, Kluwer Academic Publishers, 2008			
Consortium,e-books and Web Link references (SHOULD/ Could Know)	1. W3.org 2. Meity.gov.in 3. SIGSAC SIGSEC acm.org 4. Isca-speech.org 5. Issa.org 6. Oracle.com/database/security 7. Thelawreviews.co.uk 8. Data Security Council of India (DSCI) 9. prsindia.org 10. iso.org ISO/IEC 27000/27001/27002			

Laboratory Assignments/ Demonstrations				
LAB Assignments	*Each student will work on a unique case study. Will require approval of the same at thebeginning. Report submission is essential for each Lab Assignment.			
1	Describe the Use Case*. Model the case study. Abstract. Apply & implement DDL.	Unit-1,	02 hours	CO1
2	Using the case-study, Apply and implement the Security Model. Analyse Threats. Wrt Roles, Access Rights.	Unit-2	02 hours	CO2
3	Apply, analyse, and evaluate ACID Properties. Identify Threats and implement a Mitigation-technique to secure the data tuples.	Unit-3 & 4	02 hours	C03
4	Implement and apply Multi-dimensional DBs. Implement three basic operations: Perform Diagnostic Analysis	Unit 4 & 5	02 hours	CO3
5	Implement and apply Multi-dimensional DBs. Implement operations to observe 'what-if' analysis: Perform Predictive Analysis	Unit 4 & 5	02 hours	CO4
6	Create use case environment, Implement & Perform Audit wrt Application/Domain Control	Unit 6	02 hours	CO4
7	Create use case environment, implement & performaudit wrt Technology	Unit 6	02 hours	CO4
8	Create model and implement a security feature to demonstrate data security.	Unit-7	02 hours	CO4
9	Assigned ISO module's Study, Audit andPresentation.	Unit 1 to 7	Sem	CO4
10	Mini-project. Implementation and Demonstration. Report Submission is essential	Unit 1 to 7	Sem	CO4

Subject Code	**CS-602**
Subject title	**Machine Learning for Cyber Security**
Credit	**04**
Type of Subject	-Core (Mtech in CSE) -Professional Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	1. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 2. One Final Evaluation at the End of the Term **50 Marks** 3. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	Basic computer networking, operating systems and computer programming knowledge is required
Dept	CSE
Course Objectives	To provide the knowledge of programming language as it applies to data analytics. Skills will be developed for articulate and explain which problems in Cyber Security may be solvable with Machine Learning. Student will learn various ML techniques including Supervised, unsupervised classification and regression analysis, Artificial Neural Networks, etc. for solving Cyber Security problems such as malware analysis, intrusion detection, spam filtering, fraud detection, online

	behavior analysis etc. Student will learn Python Programming for implementing these algorithms on standard datasets to develop tools for cyber defense using machine learning.		
Course Outcomes	Bloom's Taxonomy: Level-1 Remember; Level-2 Understand; Level-3 Apply; Level-4 Analyze Level-5 Evaluate; Level-6 Create		
	CO Title	**Level**	**Descriptor**
	CO 1 – Students will be able to understand ML paradigms and various Supervised, unsupervised classification and regression analysis methods. (PO1,PO2, PO3, PSO2)	L1, L2	Remember, Learn, Understand
	CO2: Students will be able to understand various ML algorithms like and analyse their applications in real world (PO1,PO2, PO3, PSO2)	L2	Remember, Learn, Understand
	CO3: Students will be able to understand advanced ML algorithms and techniques etc. (PO1,PO2, PO3, PSO2)	L3	Remembering, Understanding, Analysing
	CO4: Students will be capable of applying their ML knowledge and skills to solve engineering problems in various domains using ML programming languages in Cyber security domain (PO1, PO2, PO3, PSO1, PSO2)	L4	Applying, Analysing

CO-PO: Course Outcome and Program Outcome Evaluation Metrics

	PO1	PO2	PO3	PSO1	PSO2
CO1					
CO2					
CO3					
CO4					

Syllabus Description

Basics & Preliminaries	**Details**	**Books & References**	**Duration**	**Cos**
Unit-1	Data Analytics Foundations: R programming, Python Basics -Expressions and Variables, String Operations, Lists and Tuples, Sets, Dictionaries Conditions and Branching, Loops, Functions, Objects and Classes, Reading/Writing files, Hand ling data with Pandas, Scikit Library, Numpy Library, Matplotlib, scikit programming for data analysis, setting up lab environment, study of standard datasets. Introduction to Machine Learning-Applications of Machine Learning, Supervised, unsupervised classification and regression analysis	Textbooks -1,2	12 Hrs	CO1
Unit-2	Python libraries suitable for Machine Learning Feature Extraction. Data pre-processing, feature analysis etc., Dimensionality Reduction & Feature Selection Methods, Linear Discriminant Analysis and Principal Component Analysis, tackle data class imbalance problem	Textbooks -2,3	12 Hrs	CO2

Unit-3	Supervised and regression analysis, Regression, Linear Regression, Non-linear Regression, Model evaluation methods, Classification, K-Nearest Neighbor, Naïve Bayes, Decision Trees, Logistic Regression, Support Vector Machines, Artificial Neural Networks, Model Evaluation. Ensemble Learning, Convolutional Neural Networks, Spectral Embedding, Manifold detection and Anomaly Detection.	Textbooks -2,3,4	12 Hrs	CO2
Unit-4	Unsupervised classification K-Means Clustering, Hierarchical Clustering, Density-Based Clustering, Recommender Systems- Content-based recommender systems, Collaborative Filtering, machine learning techniques for standard dataset, ML applications, Case studies on Cyber Security problems that can be solved using Machine learning like Malware Analysis, Intrusion Detection, Spam detection, Phishing detection, Financial Fraud detection, Denial of Service Detection.	Textbooks -4-5, / References -1-4	12 Hrs	CO3
	LAB/ Assignments/Student Presentations [2T/P per week]	Textbooks -4-5, / References -1-4	02 Hrs/Week	CO4
Text Books (MUST Know)	1. Building Machine Learning Systems with Python – Willi Richert, Luis Pedro Coelho 2. Alessandro Parisi, Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies Publication date :Aug 2, 2019, Packt, ISBN-13, 9781789804027 3. Machine Learning: An Algorithmic Perspective – Stephen Marsland 4. Sunita Vikrant Dhavale, “Advanced Image-based Spam Detection and Filtering Techniques”, IGI Global, 2017 5. Soma Halder , Sinan Ozdemir, Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem, By Publication date : Dec 31, 2018, Packt, ISBN-13 :9781788992282			
Reference Books (SHOULD Know)	1. Stuart Russell, Peter Norvig (2009), “Artificial Intelligence – A Modern Approach”, Pearson Elaine Rich & Kevin Knight (1999), “Artificial Intelligence”, TMH, 2nd Edition 2. NP Padhy (2010), “Artificial Intelligence & Intelligent System”, Oxford 3. ZM Zurada (1992), “Introduction to Artificial Neural Systems”, West Publishing Company 4. Research paper for study (if any) - White papers on multimedia from IEEE/ACM/Elsevier/Spinger/ NVidia sources.			

Laboratory Assignments/ Demonstrations

1	Python Programming part-1	Unit -1	02 hours	CO1, CO3, & CO4
2	Python Programming part-2	Unit -1	02 hours	CO1, CO3, & CO4
3	Study and Implement Linear Regression Algorithm for any standard dataset like in cyber security domain	Unit -2	02 hours	CO2, CO3, & CO4
4	Study and Implement the KMeans Algorithm for any standard dataset in cyber security domain	Unit -3	02 hours	CO1, CO3, & CO4
5	Study and Implement KNN for any standard dataset in cyber security domain	Unit -3	02 hours	CO1, & CO4

6	Study and Implement ANN for any standard dataset in cyber security domain	Unit -3	02 hours	CO2, & CO3
7	Study and Implement PCA for any standard dataset in cyber security domain	Unit -3	02 hours	CO3, & CO4
8	Case Study: Use of ML along with Fuzzy Logic/GA to solve real world Problem in cyber security domain	Unit -4	02 hours	CO2, & CO3
9	Mini assignment: Apply ML along with PSO/ACO to solve any real world problem in cyber security domain	Unit -4	02 hours	CO2, & CO4
10	ML Practice Test – 1 Quiz	Unit -1,2,3,4	02 hours	CO1,CO2, CO3, & CO4

Subject Code	CS-603			
Subject Title	**Applied Cryptography**			
Credit	**04**			
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.			
Evaluation Pattern	03 – monthly test + 01 Final Evaluation 1. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 2. One Final Evaluation at the End of the Term **50 Marks** 3. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**			
Total Marks	100			
Prerequisite	Basic understanding of mathematics concept like Prime numbers, Modulus, Operations over polynomials, Vector Algebra and knowledge of any one of the programming language(C/C++/Java/Python)			
Objective	Understanding of basic encryption and authentication schemes and issue related to cryptanalysis and be able to determine the strength and weakness of the encryption/authentication schemes.			
Course Outcome	CO1: Students are able to understand and analyse Private keys encryption schemes CO2: Public keys encryption schemes and able to perform the cryptanalysis CO3: Students are able to understand and design new schemes for information security CO4: Students are able to understand and design new schemes for end user's authentication & secure Communication			
Syllabus Details		**Book**	**Hours**	**Outcome**
Unit – 1	Classical Encryption Techniques and their Cryptanalysis: Symmetric cipher model, Substitution techniques, Transposition techniques, Steganography, One-Time Pad (Vernam's Cipher), Limitations of Perfect Secrecy, Shannon's Theorem	Text Book-1	6	CO3, & CO4
Unit – 2	Private-Key Encryption Schemes and Block Ciphers: Pseudorandom Functions and Permutations, Private-Key Encryption Schemes from Pseudorandom Functions, DES – The Data Encryption Standard, Attacks on DES, Single-Round DES, Two-Round DES, Three-Round DES, Brute Force Search, Best Known Attacks on Full DES, AES, Stream cipher A5	Text Book-1	8	CO1, & CO3
Unit – 3	Number Theory: Prime numbers and factoring, modular arithmetic, computations in finite fields, Cyclic Groups, Euclidian Algorithms, Miller-Rabin Primality Test, Chinese Remainder Theorem Discrete logarithms	Text Book-1	6	CO1, & CO3
Unit – 4	Public-Key (Asymmetric) Cryptography: Public-Key Problems and Mathematical Background, Diffie-Hellman Key Agreement, El-Gamal Encryption Scheme, RSA Encryption, Security of RSA, Hybrid Encryption , Attacks on RSA, Private and Public-Key Reversal, Common Modulus Attack, Simplified	Text Book-1	6	CO2, & CO3

	Broadcast Attack,Timing Attacks, Elliptic Curve Cryptography.			
Unit – 5	Hash Functions: Definition and Properties, Constructions of Collision-Resistant Hash Functions, Random Oracle Model. Birthday Problems, Hashalgorithms:MD5,SHA-256.Message Authentication, Digital Signatures and Applications, Definitions, Constructions, Certificates and Public-Key Infrastructure, Combining Encryption and Signatures – SignCryption.	Text Book-1	6	CO3, & CO4
Unit – 6	Homomorphic Encryption, Differential Privacy, Multiparty Computation, Functional Encryption	Text Book-4 & Research Papers	6	CO3

Textbooks:

1. "Cryptography & Network Security" by William Stallings 4th Edition, 2006, Pearson Education Asia.
2. Kahate A, "Cryptography & Network Security", Tata McGraw Hill, 2004.
3. Post-Quantum Cryptography by Daniel J. Bernstein, Johannes, Buchmann, Erik Dahmen, Springer. ISBN: 978-3-540-88701-0.
4. "Applied Cryptology" by Schiner Bruce, John Wiley & Sons

References:

1. "Applied Cryptology" by Schiner Bruce, John Wiley & Sons, 2001.
2. "Introduction to Cryptography with Coding Theory" by Wade Trappe & Lawrence C Washington, New Jersey, Pearson Education, 2006.
3. Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security: Private Communication in a Public World", Prentice Hall of India Private Limited.
4. Behrouz A. Forouzan, "Cryptography and Network Security", McGraw Hill
5. Jonathan Katz and Lindell, "Introduction to Modern Cryptography: Principles and Protocols", Chapman and Hall/CRC

Lab Assignments

Lab 1	To encrypt the text containing numbers using Playfair Cipher	Unit-1	02 hours	CO3, & CO4
Lab 2	To encrypt the image containing RGB values in the pixel using playfair	Unit-1	02 hours	CO3, & CO4
Lab 3	Programme to find the multiplicative inverse of an integer	Unit-3	02 hours	CO1, & CO3
Lab 4	Programme to find the polynomial inverse	Unit-3	02 hours	CO1, & CO3
Lab 5	Programme to implement the Key expansion of Data Encryption Standard	Unit-2	02 hours	CO1, & CO3
Lab 6	To encrypt the text file using the using A5 Stream cipher	Unit-2	02 hours	CO1, & CO3
Lab 7	Programme for Fair Coin Toss	Unit-4	02 hours	CO2, & CO3
Lab 8	Develop a system to Securely Info Exchange between 2 Ends (Mini Project)	Unit-2,3,4, 5	02 hours	CO1, & CO3
Lab 9	Develop code for symmetric key encryption.	Unit-2, 6	02 hours	CO1, & CO3
Lab 10	Light weight symmetric key encryption applications.	Unit-2	02 hours	CO1, & CO3

Subject Code	CS-604
Subject title	**Advanced System Security**
Credit	**04**
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	03 monthly tests + 01 final evaluation + assignments for internal assessment
Total Marks	100
Prerequisite	Basic Operating System concepts; Programming language- preferably C

Objective:
To learn designing and building a secure operating system, ensuring the enforcement of system security goals and evaluating the OS w.r.t necessary and sufficient conditions.
This includes learning and understanding-

- The security architectures of current operating systems
- Distinct approaches to building secure operating systems and Challenges in implementation
- Concept of virtualization
- Explore a range of existing problems and tensions in modern systems' security

Course Outcome:

CO1- Understand the System Security concept. Learn the security terminology and models. Identify the components in building a secure OS.
CO2- Analyse and Assess the security mechanisms in in earlier implemented secure OS and the contemporary commercial OS. Assess the vulnerabilities and challenges.
CO3- Learn the Security policy models. Apply the policy and mechanism to building secure operating systems based on the security goals. Analyse and evaluate the distinct approaches for Secure OS design using VM.
CO4- Practically realize the exploits of security mechanism and prevention mechanism to appreciate a Systems' security level.

Syllabus Details:	Text Book	Hours	Outcome
Unit – 1 **Security Principles:** CIA triad; Operating System Security goals, Trust model, Threat model; Protection system; Reference monitor concept. Distributed System Security Goals. **Access Control:** Discretionary protection system, Mandatory protection system, Authentication and Role Based Access Control, Authorization and Attribute Based Access Control, Rule-based access control.	Textbook1, Reference1	08	CO1, CO4
Unit – 2 **Multics:** Multics security fundamentals, protection system models, vulnerability analysis. **Security in Commercial Operating Systems:** protection system, authorization, security analysis for Unix-like and Windows OS. Security in Distributed Systems.	Textbook1, Textbook2	12	CO2, CO4
Unit – 3 **Verifiable Security Goals:** Information flow models, secrecy models, integrity models. **Secure Capability Systems:** Capability system fundamentals, Secure capability systems mechanisms. **Secure Virtual**	Textbook1, Reference2	14	CO3, CO4

Machine Systems: Separation kernels, sandboxing, Multiple Independent Levels of Security.			
Unit – 4 **Threat Vectors, Threat Intelligence,** Memory exploits, code based attacks; buffer overflow attacks; Return-to-libc, Micro-architectural attacks Spectre and Meltdown; **Hardware Security:** H/w trojans, Root of trust, Hardware based root of trust, Challenges in Bootstrapping trust in secure hardware and Trust worthy devices **Case Studies** of OS exploits & Security enhanced OS: student presentation & interactive sessions	Textbook1, Textbook2, Textbook3, Reference1 & 5	14	CO2, CO4

Textbooks

1. Jaeger, T., "Operating System Security", Morgan & Claypool (online), 2008.
2. Wenliang Du, "Computer & Internet Security: A Hands-on Approach", 1 May 2022
3. Bhunia, S., and M. M. Tehranipoor. "The Hardware Trojan War: Attacks, Myths, and Defenses. Springer, 2018."

References

1. Matt Bishop, "Computer Security", Addison Wesley, 2002
2. Morrie Gasser: "Building a Secure Computer System"
3. Silberschatz and Galvin: "Operating System Concepts", Addison Wesley, 2006
4. Virgil Gligor's Lectures on Security Policies.
5. Bootstrapping Trust in Modern Computers, Byron Parno, Jonathan M, Adrian Perrig, Springer

Lab Assignments

Lab 1	OS basics - UNIX commands	Unit 1	02 Hrs	CO1 & CO4
Lab 2	User management & Access Control in Linux & Windows	Unit 1	02 Hrs	CO1 & CO4
Lab 3	Environment Variables and SetUID	Unit 2	02 Hrs	CO2 & CO4
Lab 4	Exploring limitations of DAC in conventional Linux / Windows, exploits	Units 1 & 2	02 Hrs	CO1, CO2 & CO4
Lab 5	Buffer Overflow; Return-oriented Programming	Unit 4	02 Hrs	CO2 & CO4
Lab 6	Creating isolated environment - Jailing in Linux using "chroot", sandboxing	Unit 2	02 Hrs	CO2 & CO4
Lab 7	VM Install and Kernel Compile	Unit 3	02 Hrs	CO3 & CO4
Lab 8 – Lab 10	Mini Project: Implementing Linux Security Module || Code Injection || Binary Exploitation || Kernel Backdoors and Rootkits || Realization of (any of the) Attack Vectors	Units 1, 2, 3, 4	02 Hrs	CO1, CO2, CO3 & CO4

Subject Code	**CS-605**
Subject title	**Network and Cloud Security**
Credit	**04**
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	03 monthly tests + 01 final evaluation + assignments for internal assessment
Total Marks	100

Prerequisite	Basic computer networking, operating systems and computer programming knowledge is required.

Objective:

Understanding basic issues, concepts, principles and mechanisms in Network and Cloud Security.

- Basic Security concepts
- Authentication
- Access Control
- IPSec and Internet Key Management
- SSL/TLS Protocol
- Firewall/UTM
- Malicious Software
- Intruder Detection Systems
- Cloud Computing and Security

Be able to determine appropriate mechanisms for protecting networked systems. Network and Cloud Security Laboratory.

- To facilitate individual in gaining knowledge on Network and Cloud Security Protocols, Appliances and systems.
- To facilitate individual in gaining hands on experience on various attacks and countermeasures

Course Outcomes:

CO1: Students will be able to understand and apply Network and Cloud security Concepts along with various countermeasures. (PO1, PO3, PSO1)

CO2: Students will be able to understand and apply Network and Cloud Security concepts, hardware, software, standards and policies required for an organization. (PO1, PO2, PO3, PSO1)

CO3: Students will be able to understand the importance of implementation of Network and Cloud Security protocols, Devices, policies. (PO1, PO3, PSO1)

CO4: Students will be capable of applying their knowledge and skills to solve engineering problems in Network and Cloud Security. (PO1, PO2, PO3, PSO1, PSO2)

Syllabus:

Syllabus Details		Text Book	Hours	Outcome
Unit 1	Introduction, OSI security Architecture, Security Principles, Attacks and Threats, Model of Network Security; Security at Application Layer: Email Architecture, PGP, S/MIME	Text book 1 Chap 1, & 8	6	CO1
Unit 2	Security at Transport Layer: SSL Architecture, TLS, SET, HTTPS protocols; Security at Network Layer, IPSec, VPN, ISKMP	Text Book1, Chap 6 & 9	7	CO1
Unit 3	Firewall: Types of Firewalls, Firewall configuration, DMZ, UTMs	Text book 1 Chap 12	5	CO1
Unit 4	Intrusion Detection and Intrusion Prevention Systems, Honeypots, Distributed IDS, Password Management Authentication: kerberos, X509, Authentication, PKI	Text Book 1 Chap 11 & 4	7	CO2
Unit 5	Wireless Security: Wireless LAN, 802.11 Standards, Security of WLAN	Text Book 1 Chap 7	4	CO2
Unit 6	Cloud Security: Cloud Computing, Security Issues and Challenges, Applications	Text Book 1 Chap 5	5	CO2

Unit 7	DDoS : Direct, Reflector and Amplifier Attacks, TCP Syn Flooding, Countermeasures, Digital Attack Maps	Text Book 1 Chap 10 Text Book 2	3	CO3
Unit 8	Malicious Software: Viruses, Worms, Ransomware etc, Anti-virus Architecture, Generation of Anti-Virus, Types of Viruses; Network Reconnaissance, Traceroute, Port Scanning, ICMP Scanning, Sniffing, Probing Routers	Text Book 1 Chap 10 Text Book 3	6	CO3
Unit 9	Game Theory applications in Network Security	Research Papers	4	CO3
Unit 10	Miscellaneous topics and current developments, Dark Web Network Security Observatory: Monitoring Networks	Research Papers	7	

Text Book:

1. William Stallings, "Network Security Essentials", 6th Edition, Pearson Education, 2019.
2. B. Menezes, "Network Security and Cryptography", Cengage, 2013.
3. W. Du, "Computer and Internet Security: A Hands On Approach", 3rd Edition, 2022.

Reference Books:

1. A Fadia, "Network Security: A Hacker's Perspective", Second Edition, Macmilan, 2013.
2. Bragg et al. "Network Security: The complete Reference", McGraw Hill, 2004
3. Seedlabs: https://seedsecuritylabs.org/ (last accessed on 12th June 2022).

Lab Assignments

Sl No	Lab Experiment	Unit	Hours	Outcome
1	Packet Sniffing and Spoofing Lab	1	2 hrs	CO1, CO4
2	TCP attacks Lab	2	2 hrs	CO1, CO4
3	Firewall Exploration Lab	3	2 hrs	CO1, CO4
4	VPN Lab	2	2 hrs	CO1, CO4
5	Wireshark Lab	8	2 hrs	CO3, CO4
6	Snort: Intrusion Detection Lab	4	2 hrs	CO2, CO4
7	CyberCiege Lab	1	2 hrs	CO1, CO4
8	OpenSSL Exploration Lab	2	2 hrs	CO1, CO4
9	Digital Attack Maps DOS lab	7	2 hrs	CO3, CO4
10	Cloud Computing Lab	6	2 hrs	CO2, CO4

Subject Code	**AM 607**
Subject Title	**Mathematics for Engineers**
Credit	**04**
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	03 monthly tests + 01 final evaluation + assignments for internal assessment
Total Marks	100
Prerequisite	

Course offered from Mathematics Department, DIAT

Syllabus:

Elements of Probability and Statistics: Basic concepts of Probability, Discrete Probability Distributions (Binomial, Poisson etc.),Continuous Probability Distributions (Normal, Exponential, etc.,).

Components of Operations Research:

Introduction to Operations Research, Linear programming (Simplex Method, Revised Simplex Method, Dual simplex, Duality theory),Transportation Models.

Algebra:

General (real) vector spaces, Subspaces, Linear Independence of Vectors, Basis and Dimension, Linear Transformations, Span, Norms,Orthogonal basis and Gram-Schmidt Orthogonalization.

Ordinary Differential Equations :

Review of solution methods for first order as well as second order equations, Power Series methods. Higher Order Linear Equations,Boundary Value Problems for Second Order Equations.

Transform Techniques :

Overview of Laplace transforms, Fourier Transforms, Z transform.

Numerical Methods for ODE and P.D.E.:

Taylor series method – Euler and Modified Euler methods –

Runge-Kutta method. Parabolic, Hyperbolic and Elliptic

Equations using finite difference method

Text/References:

1. Advanced Engineering Mathematics, 11th Ed, 2010, Erwin Kreyszig, Wiley Eastern.
2. Linear Algebra and its Applications, 4th Ed., 2008, Gilbert Strang, Academic Press.
3. Numerical Methods for Scientists and Engineers, Joe D. Hoffman, Marcel Dekker Inc.
4. Numerical Methods for Engineers, Sixth Edition, Steven Chapra and Raymond Canale, McGraw-Hill Education
5. Elements of Numerical Analysis, 2nd Edition, Radhey S. Gupta**,** Cambridge University Press
6. Numerical Solutions of Partial Differential Equations: An Introduction, 2nd Ed., 2005, K. W. Morton, D. F. Mayers, CambridgeUniversity Press.
7. Operations Research: An Introduction, 9th Ed., 2010, Taha, H.A., Prentice Hall of India.
8. Optimization Theory and Applications, 2nd Ed., 1984, S.S. Rao, Wieley Eastern Ltd.
9. Introduction to probability and statistics for engineers and scientists, 4th Ed., 2009, Ross S M, Acdemic Press.
10. An Introduction to Probability Theory and its Application, 3rd Ed., 2012, William Feller, John Wiley India Pvt. Ltd.
11. Differential Equations and Dynamical Systems, Texts in Applied Mathematics, L. Perko, 3rd Ed., Vol. 7, 2006, Springer Verlag,New York.
12. .S. Gupta.. Calculus of Variation, Prentice Hall of India Pvt. Ltd.

Subject Code	PGC-601
Subject title	**Research Methodology and IPR**
Credit	**02**
Teaching Scheme	Lectures: 02 hours/week
Evaluation Pattern	03 monthly tests + 01 final evaluation + assignments for internal assessment
Total Marks	
Prerequisite	
Course Instructor	

Syllabus Contents:

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

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

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

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

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

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

References:

- Stuart Melville and Wayne Goddard, “Research methodology: an introduction for
- science & engineering students’”
- Wayne Goddard and Stuart Melville, “Research Methodology: An Introduction”
- Ranjit Kumar, 2nd Edition, “Research Methodology: A Step by Step Guide for
- Halbert, “Resisting Intellectual Property”, Taylor & Francis Ltd,2007.
- Mayall, “Industrial Design”, McGraw Hill, 1992.
- Niebel, “Product Design”, McGraw Hill, 1974.
- Asimov, “Introduction to Design”, Prentice Hall, 1962.
- Robert P. Merges, Peter S. Menell, Mark A. Lemley, “Intellectual Property in New Technological Age”, 2016.
- T. Ramappa, “Intellectual Property Rights Under WTO”, S. Chand, 2008

Subject Code	CS-611			
Subject title	**Digital Forensics**			
Credit	**04**			
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/weekTotal Contact hours 05 per week.			
Evaluation Pattern	1. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 2. One Final Evaluation at the End of the Term **50 Marks** 3. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**			
Total Marks	100 Marks			
Prerequisite	Knowledge of OS, Assembly Languages like Python, Number System and their Conversions, Internal Structure of CD/DVD.			
Course Outcomes	CO1: Students will be able to understand the standard procedures of Digital Forensics required for Cyber Crime Investigation. CO2 : Students will be able to apply proper commands and procedures required for digital investigation. CO3: Students can practically demonstrate or articulate the suspicious activity/artifacts extraction w.r.t. from the digital evidence. CO4: Students will be able to solve the real-time case-studies available on benchmarked repositories			
Syllabus Details	**Details**	**Text books/Refernce books**	**No. of Hrs**	**Cos**
Unit 1	Introduction to digital forensics Stages of Forensic: acquisition or imaging of exhibits, analysis and reporting standards Introduction to Computer Forensics: Digital Devices with rudimentary computing power Acquisition or imaging of Onboard Memory and Static Memory Introduction to legal issues, Analysis and Reporting Standards,Online and Live Forensics	Text Book1, R3	12	CO1, CO4
Unit 2	Forensic study of database and their metadata, database contents, log-files for creating timeline or recover relevant information	Text Book3	12	CO3, CO4
Unit 3	MFT & Registry Hives Extraction from Windows OS through Tools and Scripts Data Carving Using Open Source Tools,Data Recovery and Secure deletion on Storage media. Evidence or Intrusion detection from internet logs, monitoring and analysis of network traffic.Internet of Things	Text Book2, R1	12	CO2, CO4
Unit 4	Drone Forensics: Internal and External Memory Artifacts Analysis of DJI Drone Models, Study of Various Drone-Components and their Artifacts, Fly-Path Reconstruction, Directory Analysis, Telemetry Data Recovery from Internal and External Memory of particular Drone Model	Text Book2, R2	12	CO2, CO4
Text Book: 1. Kanellis, Panagiotis, “Digital Crime and Forensic Science in Cyberspace”, IGI Publishing”, ISBN 1591408733.				

2. Marshell, Angus M. (2008), “Digital Forensics: Digital Evidence in Criminal Investigation”, Wiley-Blackwell, ISBN 0470517751.
3 Brain Carrier, “File System Forensics Analysis”, Addison-Wesley Professional, 1st Edition, 2005

Reference Books:

1. Chris Prosise, Kevin Mandia “ Incident Response & Computer Forensics", McGraw-Hill, 2nd Edition, 2003.
2. Rick Ayers, Sam Brothers, Wayne Jansen, “Guidelines on Mobile Device Forensics”, NIST, US Dept. of Commerce, Revision 1, 2014
3. Pavan Duggal, “Cyberlaw–The Indian Perspective”, 2009 Edition

Lab Assignments

Name of Experiments	Units	Duration (Hrs)	Co’s
1. Perform Imaging and Analysis of Non-Volatile Memory using Open Source Tools in the absence of Write-Blockers.	I	02	CO1, CO4
2. Perform Imaging and Analysis of Non-Volatile Memory using EnCase/Other Open Source Tools With and Without Write Blockers.	I	02	CO1, CO4
3. Explore the Phases of Ethical Hacking in terms of implementing some attack.	I	02	CO1, CO4
4. Perform Imaging and Analysis of Volatile Memory using EnCase/Other Open Source Tools	I	02	CO1, CO4
5. MFT & Registry Hives Extraction from Windows OS through Tools and Scripts.	II	02	CO3, CO4
6. Recovering Deleted File from the File System	II	02	CO3, CO4
7. SystemHiding Data into Slack Space.	II	02	CO3, CO4
8. Data Recovery and Secure deletion on Storage media.	III	02	CO2, CO4
9. Data Carving Using Open Source Tools	III	02	CO2, CO4
10. Information gathering and network traffic analysis using TCP DUMP and WIN DUMP	III	02	CO2, CO4
11. Attacks and Forensics using IoT devices	IV	02	CO3, CO4
12. Social Network Artifacts Extraction and Analysis.	IV	02	CO3, CO4

Subject Code	**CS-612**
Subject Title	**Reverse Engineering & Malware Analysis**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching	Lectures: 03 hours/week

Scheme	Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	1. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 2. One Final Evaluation at the End of the Term **50 Marks** 3. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	OS fundamentals, Basics of Assembly language programming.
Dept	CSE
Course Objective	The course introduces reverse engineering techniques and further examines the use of reversing for detecting, analyzing, and eradicating malware. It involves: 1 Learning low level details of binary files and applying the reverse engineering techniques and tools to analyse any binary file without documentation. 2 Techniques to prevent binary file from reversing 3 Common vulnerabilities and protections in binary 4 Static and dynamic malware analysis
Course Outcomes	On completion of this course, the students should be able to

	CO Title	**Level**
	CO1 - Reverse engineer a binary executable file in an understandable form.	Level 2,3,4
	CO2 - Detect the vulnerabilities in the executable code.	Level 3/4/5
	CO3 - Identify the different types of malware analysis methods to recognize the binary with evasive, anti-reversing mechanism.	Level 4/5
	CO4 - Perform code analysis and recognize common malware characteristics. Setup an environment for malware analysis and perform runtime analysis. Understand and trace process execution on a system.	Level 4/5

CO-PO: Course Outcome and Program Outcome Evaluation Metrics

	PO1	PO2	PO3	PSO1	PSO2
CO1	-	-	Y	Y	-
CO2	Y	-	Y	Y	-
CO3	Y	-	Y	Y	Y
CO4	Y	Y	Y	Y	Y

Syllabus Description

Unit	**Topics**	**Text Book**	**Duration**	**COs**
Unit-1	Introduction to reverse engineering; Low level software perspective; Windows OS fundamentals; Compilers, Execution Environments; Assembly language primer; Executable file formats; Calling Conventions; Offline code analysis; Reversing tools, Disassemblers, Debuggers, Decompilers, System monitoring tools;	Text Book-1, Ch-1	16L	CO1, CO2, PO1, PO3, PSO1

Unit-2	Static or offline reversing of program binaries Dynamic reverse engineering; Debugging binary cod	Text Book-1, Ch-2, 3	10L	CO2, PO1, PO3, PSO1
Unit-3	Anti-reversing techniques, Breaking protections Reversing '.NET', De-compilation Software vulnerabilities – buffer overflow, integer overflow, vulnerabilities exploitation, mitigation; Return oriented programming;	Text Book-1, Ch-4	12L	CO2, CO3; PO1, PO3, PSO1, PSO2
Unit-4	Introduction to malware Reversing malware – Static & Dynamic malware analysis techniques Packers & compression, Sandboxing executables& runtime analysis; Fileless Malware; Malware classification STUDENT PRESENTATION & INTERACTIVE SESSIONs	Text Book-1, Ch-4, 5	10L+8T	CO3, CO4; PO1, PO2, PO3, PSO1, PSO2
Text Books (MUST Know)	1. Eldad Eilam, "Reversing: Secrets of Reverse Engineering", Wiley publishing, 2005 2. Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware, by Abhijit Mohanta (Author), Anoop Saldanha, September 2020			
Reference Books (SHOULD Know)	1. Michael Ligh, Steven Adair, "Malware Analysts's cookbook & DVD", Wiley publishing 2. Michael Sikorski and Andrew Honig, Practical Malware Analysis, No Starch Press, 2012. 3. Abhishek Singh, "Identifying Malicious Code through Reverse Engineering", Springer Publcations, 2009. ISBN No – 978-0-387-09824-1 4. Erik Buchanan, Ryan Roemer, HovavShacham, and Stefan Savage. 2008. "When good instructions go bad: generalizing return-oriented programming to RISC."			

Laboratory Assignments/ Demonstrations-

1	To explore the components of executable file in Linux and Windows.	Unit-1		CO1
2	To Debug an executable to reverse DLL using Ollydbg and IDA Pro	Unit-1		CO2
3	Dll injection	Unit-2		C03
4	IAT extraction	Unit 1 & 2		CO3
5	Usage of system monitoring tools	Unit 1,2,3,4		CO2
6	Packing and analysis of executable files	Unit 3,4		CO3
7	Find vulnerability in executable code	Unit 2,3		CO3
8	Advanced Static Analysis of Malware samples	Unit 4		CO4
9	Advanced Runtime Analysis of Malware samples	Unit 4		CO4
10	To explore the components of executable file in Linux and Windows.	Unit 2,3		CO2

11	Mini Project Statements: Hooking Detection, Keylogger Implementation and Detection, Heuristic rules for Malware Detection, Stack Smashing Attack / ROP Attack, Malware analysis & Report presentation	Unit 1,2,3,4		CO1, CO2, CO3, CO4

Subject Code	**CS-613**		
Subject Title	**Security Standards & Penetration Testing**		
Credit	**04**		
Type of Subject	-Core (MTech in CSE) -Professional Open Elective for All Engineering and Science disciplines		
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.		
Evaluation Pattern	1. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 2. One Final Evaluation at the End of the Term **50 Marks** 3. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**		
Total Marks	100 Marks		
Prerequisite	Basic computer networking, operating systems and computer programming knowledge is required.		
Dept	CSE		
Course Objectives	This course examines the methods for securing information existing in different forms. This course will provide an introduction to the different technical and administrative aspects of Information Security and Assurance. Also, one cannot protect his information assets if he doesn't know how attackers think and what techniques attackers use to exploit systems. Hence, learning offensive security techniques like Ethical Hacking and penetration testing is becoming a need of future cyber security world. Objectives are: 1. To facilitate individual in gaining knowledge on information security management systems,.2. To facilitate individual in gaining knowledge on security standards like ISO-27001 standards, TCSEC, ITSEC, Secure coding etc. 3. To train individual to become competent information security professional by learning both theoretical as well as practical ethical hacking and penetration testing knowledge base		
Course Outcomes	Bloom's Taxonomy: Level-1 Remember; Level-2 Understand; Level-3 Apply; Level-4 Analyze Level-5 Evaluate; Level-6 Create		
	CO Title	**Level**	**Descriptor**
	CO1: Students will able to identify and apply basic concepts, terminology, theories, models and methods in the field of information security management field. (PO1, PO3, PSO1)	L1, L2	Remember, Understand
	CO2: Student will able to design policies for managing information security effectively adhering to ISO-27001 standards, TCSEC, ITSEC, Secure coding practices etc. (PO1,PO2, PO3, PSO1)	L3	Remember, Understand Analyse

	CO3: Student will learn to design, implement, integrate and manage various security countermeasures/tools/mechanisms/best practices and penetration testing through hands-on activities. (PO1, PO3, PSO1) attacks like Network Intrusion, DDOS, Malware attacks are carried out successfully by attackers. (PO1, PO2, PO3, PSO1, PSO2)	L3	Remember, Understand Analyse
	CO1, 03: End semester Exam	L4	Apply, Analyse

Syllabus Details

Basics & Preliminaries	Details	Books & References	Duration	Cos
Unit-1	Introduction to Information security, Concepts, Threats, Attacks, and Assets, Security Functional Requirements, Countermeasures , Access Control Principles, Access Rights , Discretionary Access Control, Role - Based Access Control, Mandatory Access Control , Trusted Computing and Multilevel Security, Security Design Principles, Cryptographic Tools, Common Criteria for Information Technology Security Evaluation, Information security management systems (ISMS), ISO27000 and other security standards, Management responsibility, Responsibilities of Chief Information Security Officer (CISO)	Textbooks -1,2	16L	CO1
Unit-2	Security audits and assurance, Information Security Policy, Standards, and Practices, Asset Management, Human Resource Security, Security awareness training, Physical Security, Risk Management, Business continuity planning, Disaster Recovery planning, Penetration Testing Methodologies Security Assessments, Penetration Testing Methodologies, Penetration Testing Steps, Setting up own virtual ethical hacking lab for experimentation, Ethical Hacking and penetration Basics - Hacking terminology & attacks, Ethics, Legality.	Textbooks -2,3	13L	CO3
Unit-3	Phases - Reconnaissance, Scanning,Gaining access, Maintaining access, Covering tracks; Reconnaissance - Information gathering,Vulnerability research, Foot -printing, whois, DNS enumeration, Social Engineering, E - Mail Tracking,Web Spiders; Scanning & Enumeration - Sniffing techniques & tools, arp/icmp/tcp/ip host discovery, types of Scanning , Ping Sweep Techniques, Nmap, Command Switches, SYN, Stealth, XMAS, NULL, IDLE, and FIN Scansdetecting OS fingerprinting, banner grabbing, Null Sessions, SNMP/DHCP/DNS enumeration, Proxy Servers, Anonymizers, HTTP Tunneling Techniques, IP Spoofing Techniques; Cryptographic Techniques	Textbooks -2,3,4,5,6 References -1-7	9L	CO2
Unit-4	Attacking System and Maintaining Access– Password/hashcracking, NetBIOS DoS Attacks, PasswordCracking Countermeasures; escalating privileges - exploiting vulnerabilities, Buffer Overflows,Rootkits, Hiding	Textbooks -4-6, / References -1-7	10L	CO2

	FilesNTFS Stream Countermeasures, Steganography Technologies, Cover tracks and Erase Evidence, Disabling Auditing, Clearing the event Log, Malware attacks-Trojan, Backdoor, Viruses, Worms, DoS/DDoS; Attacks, Windows Hacking; Linux Hacking; Web and Database Hacking; Google Hacking; Wireless Hacking; Mobile Hacking; Penetration Testing Tools like Kali Linux, Metasploit ,Pen-Test Deliverables			
	LAB/ Assignments/Student Presentations [2T/P] per week		02L/ Week	CO4
Text Books (MUST Know)	1. Michael E Whitman, Herbert J Mattord, "Principles of Information Security", Course Technology, 3rd Edition, 2008. 2. William Stallings and Lawrie Brown, "Computer Security: Principles and Practice", 2nd edition, Pearson, 2012. 3. Krutz, R. L. & Vines, R. D., "The CISSP and CAP Prep Guide", Platinum Edition, New York, Wiley Publishing., 2006. 4. Nina Godbole, "Information Systems Security: Security Management, Metrics, Frameworks and Best Practices", Wiley India Pvt Ltd, 2012. 5. Dhavale, S. V. (2019). Constructing an Ethical Hacking Knowledge Base for Threat Awareness and Prevention (pp. 1-305). Hershey, PA: IGI Global. 6. Stuart McClure, Joel Scambray, George Kurtz, "Hacking Exposed:n/w sec secrets and solutions", Mcgraw Hill, 2012			
Reference Books (SHOULD Know)	1. Various Security Standards - ISO 27000 series published by ISO. 2. Department of Defense Standard, Department of Defense, "Trusted Computer System Evaluation Criteria", Orange Book. 3. Dieter Gollmann, "Computer Security", John Wiley and Sons, Inc., 3rd edition, 2011 4. David Kennedy, Jim O'Gorman, Devon Kearns, and MatiAharoni, "Metasploitpentest guide",No starch Press, san Francisco, 2011 5. Bastian ballman, "Understanding n/w hacks:attack and defense with python", Springer,2012 6. Rich Annings, HimanshuDwivedi, Zane Lackey, "Hacking Exposed Web 2.0", Tata Mcgraw hill Edition 7. Research paper for study (if any) - White papers on multimedia from IEEE/ACM/Elsevier/Spinger/IBM/EC-Council sources			

Laboratory Assignments/ Demonstrations

1	Study Windows Essential Tools-Part 1	Unit -1	02 hours	CO1, CO2,CO3, & CO4
2	Study Windows Essential Tools-Part 2	Unit -1	02 hours	CO1, CO3, & CO4
3	Study Sysinternals utilities to manage, diagnose, troubleshoot, and monitor a Microsoft Windows environment	Unit -2	02 hours	CO2, CO3, & CO4
4	Study passive information gathering tools.	Unit -3	02 hours	CO1, CO3, & CO4
5	Write Security Policy Document	Unit -3	04 hours	CO1, & CO4
6	Case study: LDRA and Parasoft tools	Unit -3	02 hours	CO2, & CO3

7	Kali Linux Attacks – Part1	Unit -3	02 hours	CO3, & CO4
8	Kali Linux Attacks – Part2	Unit -4	04 hours	CO2, & CO3
9	SSPT Practice Test -1Quiz	Unit -4	04 hours	CO2, & CO4
10	Apply data mining tools for cyber security related data analysis	Unit -4	02 hours	CO1,CO2, CO3, & CO4

Subject Code	**CE695A**
Subject Title	**Cyber Physical Systems**
Credit	**04**
Type of Sub	Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	1. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 2. One Final Evaluation at the End of the Term **50 Marks** 3. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	None. First 10 hours will be devoted for Prerequisite learnings related to basics of Databases (04 hours), Computer Networks (02 Hours), Operating System (02 Hours), Trends in evolutions of Compute-Devices (02 Hours)
Dept	CSE
About the Course	1. This course examines a new class of computational systems called Cyber-Physical Systems CPS. Such systems have the potential to provide far-reaching benefits in addressing some of the toughest problems we face as a society, such as: reducing healthcare costs, minimizing traffic congestion, and constructing zero-net energy buildings. Four important features characterize CPS: their ability monitors the underlying physical environment, reason about the monitored data, control the physical environment through actuation, in a coordinated manner using a communication medium. It can be seen in CPS, the computational 2. element (cyber) and the environment (physical) are tightly coupled, with one influencing the other. 3. CPS sits at the confluence of several traditional disciplines, such as: embedded systems, real-time systems, sensor networks, control and hybrid systems, and security. It presents many challenging problems and opportunities for research. With guidance from the professor, students will survey recent CPS publications, develop an aptitude. 4. Readings will include papers on CPS applications (e.g., Body Area Networks, smart automobiles, and energy-efficient buildings), issues involved in designing CPS (e.g., monitoring, communication, and control), and how to ensure that the designed systems satisfy certain essential properties (e.g., safety and security).

	5. CPS combine cyber capabilities (computation and/or communication) with physical capabilities (motion or other physical processes). Cars, aircraft, and robots are prime examples, because they move physically in space in a way that is determined by discrete computerized control algorithms. Designing these algorithms to control CPSs is challenging due to their tight coupling with physical behavior. At the same time, it is vital that these algorithms be correct, since we rely on CPSs for safety-critical tasks like keeping aircraft from colliding, its role in Command & Control environments. 6. To meet end-user, Administrator & System Designer perspectives, develop skill sets to be resourceful in knowledge & information systems. Enhance analytical capabilities to evaluate a domain specific and technical area. Multi-Disciplinary Course useful to any engineering discipline who are keen to contribute in digitization, like be it smart cities, smart telemedicine systems, automated and autonomous systems.
Course Outcomes	Bloom's Taxonomy: Level-1 Remember; Level-2 Understand; Level-3 Apply; Level-4 Analyze Level-5 Evaluate; Level-6 Create

	CO Title	**Level**	**Descriptor**	**Out come**
	CO1: Students will be able to understand the scope of applications of CPS.	L1, L2	Remember, Learn, Understand	20%
	CO2: Students will be able to analyse the various components of CPS	L3, L4	Apply, Analyse	20%
	CO3: Students will apply mechanisms to enable autonomous and self-organising techniques	L4, L5	Analyse, Evaluate	20%
	CO4: Students will be capable of applying their knowledge and skills to solve engineering problems in cyber and information security domain along with scope to apply AIML and build secure digitized systems. (PO1, PO2, PO3, PSO1, PSO2)	L5, L6	Evaluate, Create	40%

Summary of the Course Out Come	At the end of the course, a student will understand the concepts of CPS. Develop skills to relate a CPS as a feedback system along with its designing, modelling and implementation challenges. Evaluate the requirements to address emerging areas of digitization, AIML, and Secure environments.

Syllabus Description

Basics & Preliminaries	Role of Basic and Advanced Data Structures in Data Models, Types of Data Models, Basic Dictionary Data Types; Algorithms and basics of analysis, OS & Algorithms in Parallel Environments. Protocols of Computer Networks Preliminaries, Concerns for Data Security and Privacy	Cormen et al,Horowitz Sahani, BipinDesai, Korth et al. Kurose Ross	10 Hours	CO1, PO1
Unit-1	CPS**:** Introduction Main Concepts, Challenges; Background role of Computer Networks, Data, Algorithms	Text Book-1, Ch-1	08 Hours	CO1, CO2, PO1

Unit-2	Self-organising Systems, Self-organisation in Natural Systems Inspiring Self-organising Software,	Text Book-1, Ch-2, 3	04 Hours	CO1, PO1
Unit-3	Agents and Multi-Agent Systems Computing trends, Data device proliferation, Confluence of trends	Text Book-1, Ch-4	06 Hours	CO1 CO2, PO1
Unit-4	Technological and economic drivers Self-organisation Mechanisms, Stigmergy, Gossip, Trust and Reputation for Successful Software Self-organisation, Cooperation , Immune Systems, Holonic Multi-Agent Systems Engineering Artificial Self-organising Systems	Text Book-1, Ch-4, 5	06 Hours	CO3, PO2
Unit-5	Engineering Self-organising Systems, Middleware Infrastructures for Self-organising Pervasive Computing Systems	Text Book-1, Ch 5,6,7,8	06 Hours	CO3, PO2
Unit-6	CPS design Standards, Time Models, CPS Special Interest Groups and Mitre Commendations in Design and developments	Weblink References	06 Hours	C04, PO4
Unit-7	Applications of Self-organising Software, Self-organisation in Constraint Problem Solving, Adaptive Trust Management, Security in Artificial Systems Project Cases: SCADA, Industry 4.0 applications, Telemedicine, Environment Monitoring, IoTs, etc.	Text book-1, Ch-8,9	06 Hours	CO1, CO4, PO1, PO3
Text Books (MUST Know)	Text Books 1. Self-Organising Software from Natural to artificial Adaptation, Di- MarzoSerugendo, ;Gleizer, M-p; Karageorgos, A (Eds), 2011, XVIII,462P; Hardcover ISBN:978-3642-17347-9		Must Know	
Reference Books (SHOULD Know)	Reference Book-1 1. "Principles of Cyber-Physical Systems" - Rajeev Alur, MIT Press, 2015 2. Data Mining, Jiawei Han & Micheline Kamber, 2nd edition, Elsevier, 2006 3. Kurose and Ross, Top Down Approach of Computer Networks, Prentice Hall, 8th Edition 2021.		Should Know	
Consortium, e-books and Web Link references	1. https://iveybusinessjournal.com/publication/why-big-data-is-the-new-competitive-advantage/https://www.cdsaonline.org/cps-standard/		Should and May know	

(SHOULD/ Could Know)	2. https://pages.nist.gov/cpspwg/ 3. International Association for Automation 4. Research Papers shared by the subject incharge			

Laboratory Assignments/ Demonstrations

LAB Assignments	*Each student will work on unique case study. Will require approval of the same at the beginning. Report submission is essential for each Lab Assignment.			
1	Describe the Use Case*. Model the case study. Abstract.	Unit-1	02 hours	CO1
2	Modelling Tools exploration and implementation of the subsystems/ systems of the case study.	Unit-2	02 hours	CO2
3	Depiction of Agents in the designed model, and modelling their state, transitions and parameters status. Any one scenario for automous execution using algorithms.	Unit-3 & 4	02 hours	C03
4	Implement and apply Multi-Agent Systems. Enumerate the challenges, risks and mitigations.	Unit 4 & 5	02 hours	CO3
5	Implement and apply Multi-Agent Systems. Enumerate the challenges, risks and mitigations. Develop the methods to audit and parameters of importance. Generate the incidence response reports.	Unit 4 & 5	02 hours	CO4
6	Implement and apply Multi-Agent Systems. Enumerate the challenges, risks and mitigations. Specify the security concern and mitigation technique. Generate the incidence response reports.	Unit 6	02 hours	CO4
7	Create use case environment, implement & perform intra and Inter-system mappings.	Unit 6	02 hours	CO4
8	Create model and implement any one security feature to demonstrate cyber security concern, intra and inter and mitigation.	Unit-7	02 hours	CO4
9	Study of Research paper on the assigned topic and its presentation.	Unit 1 to 7	Sem	CO4
10	Mini-project. Implementation and Demonstration. Report Submission is essential	Unit 1 to 7	Sem	CO4

Subject Code	CE 70G
Subject title	**Blockchain Technology**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	4. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 5. One Final Evaluation at the End of the Term **50 Marks** 6. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	Expertise in Programming, Basic Knowledge of Computer Security, Cryptography, Networking.
Dept	CSE
Course Objective	Blockchain is an emerging technology platform for developing decentralized applications and data storage, The basic tenet of this platform is that it allows one to create a distributed and replicated ledger of events, transactions, and data generated through various IT processes with strong cryptographic guarantees of tamper resistance, immutability, and verifiability. The technology itself holds much more promise in various areas such as time stamping, logging of critical events in a system, recording of transactions, trustworthy e-governance etc. Many researchers are working on many such use cases such as decentralized public key infrastructure, self-sovereign identity management, registry maintenance, health record management, decentralized authentication, decentralized DNS, etc. Considering the need to disseminate the emerging concepts for students, we proposed a new course on blockchain technology, includes the fundamental design and architectural primitives of Blockchain, the system and the security aspects, along with various use cases from different application domains
Syllabus Description	
Unit-1	Basic Cryptographic primitives used in Blockchain – Secure, Collison-resistant hash functions, digital signature, public key cryptosystems, zero-knowledge proof systems
Unit-2	Basic Distributed System concepts – distributed consensus and atomic broadcast, Byzantine fault-tolerant consensus methods.
Unit-3	Basic Blockchain – concepts to Bitcoin and contemporary proof-of-work based consensus mechanisms, operations of Bitcoin blockchain, crypto-currency as application of blockchain technology
Unit-4	Ethereum Blockchain: Samrt Contract, Introduction to Solidity Language, Proof of stake, Ethereum Network
Unit-5	Hyperledger fabric platform- Decomposing the consensus process , Hyperledger fabric components, Chaincode Design and Implementation Hyperledger Fabric
Unit-6	IoTA : Formation of Tangle, Cumulative weight, Consensus in IoTA, Double Spending Attack.
Unit-7	Beyond Cryptocurrency – applications of blockchain in cyber security, integrity of information, E-Governance and other contract enforcement mechanisms
Unit-8	Security and Research Aspects

Reference Books (SHOULD Know)	1. Bitcoin and Cryptocurrency Technologies by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, Princeton University Press 2. "S. Shukla, M. Dhawan, S. Sharma, S. Venkatesan, 'Blockchain Technology: Cryptocurrency and Applications', Oxford University Press. 3. Josh Thompson, 'Blockchain: The Blockchain for Beginnings, Guild to Blockchain Technology and Blockchain Programming', Create Space Independent Publishing Platform.

Subject Code	**CE 66A**
Subject title	**Algorithmic Cryptanalysis**
Credit	**04**
Course Objectives	This course discusses cryptanalysis from basics to advanced application from algorithmic point of view. After completion of the course, the students should be able to identify and apply the suitable algorithm for more sophisticated cryptographic applications, including LFSR-based stream ciphers and index calculus methods. The students should be able to observe the advancements in current computer architectures and its impact on implementation aspects of cryptanalysis methods.
Prerequisite	Preferred if subjects related to cryptography and algorithms are studied in graduation or semester-I.
Pre-requisite training	One week training on basics of Cryptography & algorithms.
Syllabus Description	
UNIT-I	Preliminaries, Defining security in cryptography, Elementary Number Theory and Algebra, Evolution in Computing Devices, Evolution in Communication Media, Evolving Programming Environments, Three Generic Forms of Cryptanalysis: Cipher text only, Known cipher text/plain text pairs, and Chosen plain text or chosen cipher text.
UNIT-II	General Approaches to Cryptanalysis – (i) based on properties on encryption algorithms & (ii) bruteforce, Linear Algebra, Sieve Algorithms, Brute Force Cryptanalysis, The Birthday Paradox: Sorting or Not? Birthday-Based Algorithms for Functions, Algorithmic complexities & computational costs.
UNIT-III	Birthday Attacks through Quadrisection, Fourier and Hadamard–Walsh Transforms, Lattice Reduction, Polynomial Systems and Gröbner Bases Computations; Study of protocols for cryptanalysis**.**

UNIT-IV	Attacks on Stream Ciphers, Lattice-Based Cryptanalysis, Elliptic Curves and Pairings, Index Calculus Algorithms
Text Book	1. Joux, A. (2009). Algorithmic Cryptanalysis (1st ed.). Chapman and Hall/CRC. https://doi.org/10.1201/9781420070033 2. Mihailescu, Marius Iulian, and Stefania Loredana Nita. *Pro Cryptography and Cryptanalysis: Creating Advanced Algorithms with C# and. NET*. Apress, 2021.
Reference Books	1. Gaines, Helen F. *Cryptanalysis: A study of ciphers and their solution*. Courier Corporation, 2014. 2. Wagstaff Jr, Samuel S. *Cryptanalysis of number theoretic ciphers*. Chapman and Hall/CRC, 2019. 3. Derbez, Patrick. Tools and Algorithms for Cryptanalysis. Diss. Université Rennes 1, 2022. 4. Petrenko, Alexei. Applied Quantum Cryptanalysis. CRC Press, 2023.

Course Code: CE606A

Course Title: Software Engineering & System Modelling

Credit: 4

Evaluation Pattern - 03 – monthly test + 01 Final Evaluation

Prerequisite: C programming and debugging concepts, basic concepts of operating systems.

Objective: Major objective is to learn basic principles of Software Engineering and Design, which can facilitate the resource efficient model of the Software Systems.

Course Outcome-

CO1: Students are able to understand Basic Principles of Software Engineering and Design

CO2: Students are able to create Use Cases and develop Use Case Models of the Systems.

CO3: Students are able to apply UML design notations to develop the software systems

CO4: Able to recognize and apply appropriate software design patterns for software efficiency

Unit	Syllabus Details	Outcome
Unit – I	Software Development Process, Planning software project, Cost, Scheduling and Risk Management. Metrices, Design Principles, Introduction to Object Oriented Design.	CO1, & CO4
Unit – II	Introduction to OOAD –What is OOAD? –What is UML? What are the Unified process(UP) phases, Case study –the NextGen POS system, Inception-Use case Modeling, Relating Use cases– include, extend and generalization. . Elaboration - Domain Models, Finding conceptual classes and description classes, Associations, Attributes, Domain model refinement –Finding conceptual class hierarchies, relationships, UML activity diagrams and modeling	CO2, & CO3

Unit – III	System sequence diagrams (SSD) -Relationship between sequence diagrams and use cases Logical architecture and UML package diagram, Logical architecture refinement, UML class diagrams, UML interaction diagrams	CO3, & CO4
Unit – IV	GRASP: Designing objects with responsibilities –Creator, Information expert, Low Coupling, Controller, High Cohesion, Designing for visibility, Applying GoF design patterns –adapter, singleton, factory and observer patterns.	CO1, & CO4
Unit – V	UML state diagrams and modeling -Operation contracts, Mapping design to code, UML deployment and component diagrams.	CO2, & CO4

Textbooks:

1. Software Engineering- Pankaj Jalote, TMH
2. Software Engineering- Ian Sommerville , Pearson
3. Craig Larman, "Applying UML and Patterns: An Introduction to object-oriented Analysis and Design and iterative development", Third Edition, Pearson Education

References:

1. Mike O'Docherty, "Object-Oriented Analysis & Design: Understanding System Development with UML 2.0", John Wiley & Sons, 2005.
2. 2. James W-Cooper, Addison-Wesley, "Java Design Patterns –A Tutorial", 2000.
3. 4. Erich Gamma, Richard Helm, Ralph Johnson, John Vlissides, "Design patterns: Elements of Reusable object-oriented software", Addison-Wesley, 1995.

Lab Assignments	
Lab 1	UML Modelling UML modelling through Case study: Generation of Use-case diagram, class diagram, sequence diagram.
Lab 2	Use Case Modelling
Lab 3	Security Use Cases Modelling
Lab 4	Identification of objects from Use Cases
Lab 5	Object Modelling
Lab 6	Activity Diagrams
Lab 7	Sequence Diagrams
Lab 8	Mapping of operations in Class and Sequence Diagrams
Lab 9	Implementations of Design Patterns

Subject Code	**CE 681**
Subject title	**Mobile Computing**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.

Evaluation Pattern	7. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 8. One Final Evaluation at the End of the Term **50 Marks** 9. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	Students are required to gain knowledge of basics of computer networking.
Dept	CSE
Course Objective	Course provides introduction to the fundamentals of mobile computing, mobile application development as well as wireless communication and security. Students will gain a sound understanding of the core concepts of mobile networks and the design of cellular networks including approaches to maximize the available capacity. The course will look at some current research in mobile computing security and wireless security. Students will learn android application development framework and use it to implement their assignments
Syllabus Description	
Principle of Cellular Communication, Overview 1G, 2G, 3G, 4G, LTE, 5G technologies. Wireless Transmission: Frequencies for radio transmission, Signals, Antennas, Signal Propagation, Multiplexing. Modulation, Spread spectrum, Cellular systems. Medium Access Control: Motivation for a specialized MAC, SDMA, FDMA, TDMA, CDMA, Comparison. GSM: Cellular Systems, Mobile Services, System Architecture, Radio Interface, Protocols, Localization and calling, Handover, Security. Data services: GPRS, HSCSD Mobility management: Handoff, Roaming Management, Handoff Detection Strategies, Channel Assignment, Radio Link transfer, GSM Location Update, Mobility Databases, Failure Restoration, VLR Overflow Control. Satellite Systems: GEO, LEO, MEO, Routing, Localization, Handover. Wireless LAN: Infrared and radio transmission, Infrastructure and Ad-hoc network, IEEE 802.11, Bluetooth. Mobile Device Platforms: Mobile OS, Palm Os, Win CE and Symbian. Mobile Network Layer: Mobile IP, Mobile Ad-hoc Networks, Cellular Digital Packet Data (CDPD), Wireless Local Loop (WLL) systems. Mobile Transport Layer: Traditional TCP, Classical TCP Improvements, Mobile-TCP. Wireless Application Protocol (WAP): WAP Architecture, Wireless Markup Language (WML), WML-Script, WAP 2.0. Wireless Network Security: IEEE 802.11 Wireless LAN Attacks, Different Attack Tools, Different Types of Security Mechanisms, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access –II (WPA-2), Deploying Secure Wireless networks, Security in Bluetooth, Security in Adhoc Networks. Case Study: Android Application Development, Android Security.	
Reference Books (SHOULD Know)	1. Jochen Schiller, "Mobile Communication", 2nd Edition, Pearson Education. 2. Yi Bing Lin and ImrichChlamtac, "Wireless and Mobile Networks Architecture", John Wiley & sons, 2001. 3. Ed Burnette, "Hello Android", Pragmatic Bookshelf; Third Edition edition, 2010. 4. Yan Zhang, Jun Zheng, Miao Ma, —Handbook of Research on Wireless Security‖, Volume 1, Idea Group Inc (IGI), 01-Jan-2008. 5. Raj Kamal, —Mobile Computing‖, illustrated edition, Oxford University Press, Oxford higher education, 2007.

Subject Code	**CE 683**
Subject title	**Information Warfare**

Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	10. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 11. One Final Evaluation at the End of the Term **50 Marks** 12. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	Students are required to gain knowledge of basics of computer networking.
Dept	CSE
Course Objective	This course will help students in gaining the knowledge of information warfare domain concepts including principles of information warfare (IW), Cyber warfare (CW), Offensive and defensive IW, military espionage, economic espionage, communications eavesdropping, computer break-ins, Open source intelligence, Covert Communication, Surveillance, ethical and legal concepts in the context of CW, Command and Control, Psyops and perception management. They will learn about different countermeasures, ethical hacking tools and techniques. They will form two teams (Red and Blue). One team carries out offensive operations against the; while other team will carry out defensive operations to protect the same information systems.
Syllabus Description	
Introduction to Information Warfare, Principles of Information Warfare, Conventional Warfare vs. Cyber Warfare, Information Warfare Elements (Information, Media, Computing Facilities, Communication Network, Operations, Warriors/Human Factors), Offensive and Defensive Information Warfare Operations, National Security Threats from State and Non-state Actors, Cyber-Terrorism, Information Warfare Policy, International Laws Governing Information Warfare, Law of War and Cyber Attack, Edward Snowden Revelations, ANT Catalogue, Supply Chain Risks, Open Sources, Open Source Intelligence (OSINT), Active Cyber Defenses, Competitive Intelligence, Piracy and Intellectual Property Rights, Watermarks, Steganography, Covert Communication, Privacy Protection, Subversion Techniques, Psyops and Perception Management, Military Deception, Espionage and Signals Intelligence, Insider Threat, Economic, Corporate, and Military Espionage, Traffic Analysis, Packet Sniffing, Keystroke Monitoring, Environmental Surveillance, Computer Hacking and Cybercrime, Hacking Tools and Techniques, Attacks (Denial of Service, Spoofing, Masquerade, Identity Theft, Trojan Horses, Viruses, Worms, Fraud, Physical Destruction), Security Measures (Anonymity, Sanitization, Trash Disposal, Shielding, Biometrics, Location based Authentication, Digital Signatures, Access controls, Surveillance), Communications Intercepts, Electronic Warfare, Command and Control, C4ISR, Network Centric Warfare, Wireless Security, Adhoc Network Mechanisms for Net Centric Operations, Information Warfare Case studies.	
Text Books & Reference Books (SHOULD Know)	1. Wg Cdr MK Sharma, —Cyber Warfare: The Power of Unseen‖, KW Publishers, New Delhi, 2011. 2. Emory A. Anderson, Cynthia E. Irvine, and Roger R. Schell, Roger R,.; —Subversion as a Threat in Information Warfare‖, http://calhoun.nps.edu/bitstream/handle/10945/7123/04paper_subversion.pdf 3. Philip A. Myers, —Subversion: The Neglected Aspect of Computer Security‖, Phd Thesis, Naval Postgraduate School, California, June 1980, http://csrc.nist.gov/publications/history/myer80.pdf 4. Dr. Roger R. Schell, —Information Security: Science, Pseudoscience, and Flying Pigs‖, https://www.acsac.org/invited-essay/essays/2001-schell.pdf

Subject Code	CE 689
Subject title	**Fault-Tolerant Computing System**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	13. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 14. One Final Evaluation at the End of the Term **50 Marks** 15. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	Students are required to gain knowledge of basics of computer networking.
Dept	CSE
Course Objective	
Syllabus Description	
1. Introduction: Motivation, System view of high availability design, Terminology 2. Hardware redundancy: Basic approaches, Static & Dynamic, Voting, Fault tolerant interconnection network. Application: FTMP 3. Error detection techniques: Watchdog processors, Heartbeats, Consistency and capability checking, Data audits, Assertions, Control-flow checking Application: DHCP 4. Software fault tolerance: Process pairs, Robust data structures, N version programming, Recovery blocks, Replica consistency & reintegration, Multithreaded programs Application: HP Himalaya Servers 5. Network fault tolerance: Reliable communication protocols, Agreement protocols, Database commit protocols Application: Distributed SQL server 6. Practical steps in design of high availability networked systemsApplication: Web services, Highly available clusters 7. Check pointing& Recovery Application: Microcheckpointing 8. Attack dimension to failures, byzantine generals problem, in context of side-channel attacks study fault induced leads to catastrophic failure 9. Case Studies	
Text Books & Reference Books (SHOULD Know)	1. Koren and C. Mani Krishna, Fault-tolerant Systems, 1st edition, 2007, Morgan Kaufmann. 2. D. P. Siewiorek and R. S. Swarz, Reliable Computer Systems - Design and Evaluation, 3rd edition, 1998, A.K. Peters, Limited. 2. D. K. Pradhan, ed., Fault Tolerant Computer System Design, 1st edition, 1996, Prentice-Hall.

Subject Code	CE 690
Subject title	**Parallel And Distributed Systems**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	16. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 17. One Final Evaluation at the End of the Term **50 Marks** 18. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	CSE, IT, ECE, EE, Robotics, Instrumentation Engg, Industrial Engineering, Modelling & Simulations, Fundamental Computer architecture, programming environments, computer networks
Dept	CSE
Course Objective	To meet end-user, Administrator & Designer perspectives. Enhance analytical capabilities to evaluate a system
Syllabus Description	
Unit I: Introduction to various Network Enabled Operations, Network Centric Operations, n-tier, P2P Systems; State of Art Examples and their types: GIS systems, MIS systems, Nature of Parallelism and Distributed Environment Models. **Unit II:** Parallel Architecture, Parallel Algorithms, Parallel Databases, Distributed Architecture, Distributed Systems, Distributed Databases **Unit III**: Systems modeling and Virtualization, Clusters for Scalable Parallel Computing, Virtual Machines, Virtualization Of Clusters **Unit IV:** Data Centers, Computing Clouds, Service-Oriented Architectures, Service-Oriented Architectures for Distributed Computing **Unit V:** Cloud Programming and Software Environment, Grids, P2P, Future Internet, Peer-To-Peer Computing and Overlay Networks, Ubiquitous Cloud and Internet of Things. Fog and Edge Computing. **Unit VI:** Adhoc Distributed & Self-Organising Environments, Pervasive and Ubiqutious Computations, Environments	
Text Books & Reference Books (SHOULD Know)	1. Kai Hwang, Geoffrey C. Fox, and Jack J. Dongarra, —*Distributed and Cloud Computing: From Parallel Processing to the Internet of Things*‖, MorganKaugmann Publications, 2012 2. Hwang, Kai, and Zhiwei Xu. *Scalable parallel computing: technology, architecture, programming*. McGraw-Hill, Inc., 1998.

Subject Code	CE 688
Subject title	**Game Theory**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.

Evaluation Pattern	19. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 20. One Final Evaluation at the End of the Term **50 Marks** 21. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	Basic understanding of Computer Networking and Network Security
Dept	CSE
Course Objective	To understand the concepts of Game Theory and get an overview. To learn and appreciate the applications of game theory in Network Security

Syllabus Description

Network Security Concepts: Networks and Security Threats, Networks and World Wide Web, Security Threats, Attackers, Defenders, and their Motives, Attackers, Defenders, Defense Mechanisms, Security Tradeoffs and Risk Management, Security Tradeoffs, Security Risk Management, **Introduction to Game Theory**: What is Game Theory? Game Theory Classification, Introduction to Non-Cooperative Game Theory, General Formulation for Non-cooperative Games, Existence of Nash and Saddle-Point Equilibria in Finite Games, Existence and Uniqueness of Equilibria in Infinite Games, Prisoner's Dilemma, Co-operative Game Theory, Shapley Value, **Deterministic Security Games**: Security Game Model, Intrusion Detection Games, Matrix Games, Games with Dynamic Information, Sensitivity Analysis, 160

Modeling Malicious Behavior in Social Networks, Security Games for VehicularNetworks, Vehicular Network Model, Attack and Defense Model, Game Formulation and Numerical Analysis, Security Games in Wireless Networks, Random Access Security Games,Interference Limited Multiple Access Security Games, Revocation Games, Discussion and Further Reading, **Stochastic Security Games**: Markov Security Games, Markov Game Model, Solving Markov Games, Stochastic Intrusion Detection Game, Security of Interconnected Systems, Analysis of an Illustrative Example, Linear Influence Models, Malware Filter Placement Game, Stochastic Game Formulation, Simulations. **Decision Making for Network Security**, **Security Risk Management** , Quantitative Risk Management, Risk in Networked Systems and Organizations, A Probabilistic Risk Framework, Dynamic Risk Mitigation AndControl, Security Investment Games, Influence Network and Game Model, Equilibrium and Convergence Analysis, Incentives and Game Design, Cooperative Games for Security Risk Management, Coalitional Game Model, Coalition Formation under Ideal Cooperation**Resource Allocation for Security:** An Optimization Approach To Malware Filtering, Traffic Centrality Measures, Filtering Problem Formulations, A Robust Control Framework for Security Response, Network Traffic Filtering Model, Derivation of Optimal Controller and State Estimator, Optimal and Robust Epidemic Response, Epidemic Models, Feedback Response for Malware Removal, Multiple Networks, **Machine Learning for Intrusion and Anomaly Detection:** Intrusion and Anomaly Detection, Intrusion Detection and Prevention Systems, Open Problems and Challenges, Machine Learning for Security: An Overview, Overview of Machine Learning Methods, Open Problems and Challenges, Distributed Machine Learning, SVM Classification and Decomposition, Parallel Update Algorithms, Active Set Method and A Numerical Example, Behavioral Malware Detection.

Text Books & Reference Books (SHOULD Know)	1. T. Alpcan and T. Basar, —Network Security: A decision and Game Theoritic Approach‖, Cambridge University Press. 2. M. Osborne, —AN Introduction to Game Theory‖, Oxford University Press, 2003. **Reference Books:** 1. Bragg et al, — Network Security: The complete Reference‖, McGraw Hill Osborne, 2003. 2. B. Singh, —Network Security and Management‖, Third Edition, PHI, 2013. 3. B.A. Forouzan and D. Mukhopdhyay, —Cryptography and Network Security‖, 2nd Edition, McGraw Hill, 2010. 4. A. Dixit et al., —Games of Strategy‖, Third Edition, W Norton Publishers, 2009.

Subject Code	CE 690
Subject title	**Trustworthy Computing**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	22. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 23. One Final Evaluation at the End of the Term **50 Marks** 24. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	Basic understanding of Boot Process, Shell Programming and Formal Methods, Fundamentals of OS.
Dept	CSE
Course Objective	Understanding of TPM capabilities, as well as other trusted computing standards and technologies Secure/Trusted/ Verified Boot Remote Attestation Use of open source tools for development of trusted process Be able to maintain and to develop trusted systems
Syllabus Description	
Introduction to trusted computing, Techniques for recording platforms state: Recording code identity, Recording dynamic properties. Use of platform information: Secure boot, Storage access control based on code identity. Information from platform states. Roots of trust: General-purpose tamper- resistant and Tamper-responding devices, General –purpose devices without dedicated physical defenses, Special-purpose minimal devices, Research solutions without hardware support. Challenges in bootstrapping trust in secure hardware: Problem definition, Potential solutions. Validating the process. Implementing trust bootstrapping: Open source tools. Human factors & usability, Limitations: Load-time versus run-time guarantees , Hardware attacks.	
Text Books & Reference Books (SHOULD Know)	1. Bryan ParnoJonathan M. McCune, Adrian Perrig, —Bootstrapping trust in ModernComputers‖, Springer Briefs in ComputerScience. 2. D.Challener,K.Yoder,R.Catherman,D.Safford,andL.vanDoorn,—APracticalGuide toTrusted Computing‖, IBM Press, 2008. 3.DynamicsofaTrustedPlatform:ABuildingBlockApproach,DavidGrawrock,IntelPress;1stedition, SBN:1934053171

Subject Code	CE 692
Subject title	**Computational Geometry and Applications**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	25. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 26. One Final Evaluation at the End of the Term **50 Marks**

	27. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	The students are assumed to have a basic knowledge of the design and analysis of algorithms and data structures. No knowledge of the application domains is required, and hardly any knowledge of geometry. The analysis of the randomized algorithms requires very elementary knowledge of probability theory
Dept	CSE
Course Objective	

Syllabus Description

Geometric primitives, Line intersection, randomized incremental concepts, Triangulation and visibility, Linear programming in two and three dimensions, Orthogonal range searching, Point location and Binary Space Partitions, Voronoi diagrams and Delaunay triangulation, Convex hulls, Non-orthogonal range searching

Text Books & Reference Books (SHOULD Know)	1. *Computational Geometry: Algorithms and Applications*‖, Third Edition (March 2008),Mark de Berg, TU Eindhoven (the Netherlands), Otfried Cheong, KAIST (Korea), Marc van Kreveld, Mark Overmars, Utrecht University (the Netherlands), Springer-Verlag

Subject Code	**CE 698**
Subject title	**Multimedia Security**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	28. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 29. One Final Evaluation at the End of the Term **50 Marks** 30. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	Basic computer programming knowledge is required
Dept	CSE
Course Objective	1. To facilitate individual in gaining knowledge on digital watermarking, steganographic and encryption techniques on multimedia signals like image, audio and video for digital rights management applications. 2. To facilitate individual in gaining knowledge on forensics on multimedia signals like image, audio and video for multimedia tamper/forgery detection applications. 3. To teach biometric security concepts. Student will learn and implement various algorithms using MATLAB, Python during hands-on activities carried in the Laboratory.

Syllabus Description

Steganaography and Steganalysis; Information Hiding, Digital Watermarking – Basics of host Image/Video/Audio signals, Multimedia compression and decompression, Lossless compression, Models of watermarking, watermark

detection by correlation; message coding, Mapping message in message vectors, Error correction coding, Detecting multi-symbol watermarks, Watermarking with side information, Informed embedding, Informed coding; Structured dirty-paper codes, Analyzing errors, Message errors, ROC curves, The effect of whitening on error rates, Analysis of normalized correlation, Using perceptual mode, Evaluating perceptual impact of watermarks; General forms of perceptual model, Perceptual adaptive watermarking, Robust watermarking, Spread Spectrum Watermarking, DCT-Domain Watermarking, A Buyer-Seller Watermarking Protocol, Text/Image/Video/Audio watermarking, Watermark security and cryptography, Content authentication, Applications: Digital Right Management Products & Laws, copyright protection; traitor tracing; tamper proofing; copy control; Signal processing attacks. Machine learning approaches in multimedia security, Intelligent Techniques for watermarking. Multimedia Encryption, Image/audio/video Forensic and forgery detection, Biometric Security-Introduction to Biometrics, Fingerprint Recognition, Face Recognition, Iris Recognition, Hand Geometry Recognition, Gait Recognition, The Ear as a Biometric, Voice Biometrics, A Palm print Authentication System, Online Signature Verification; Introduction to Multi biometrics, Multi biometrics Using Face and Ear, The Law and the Use of Biometrics, Biometric System Security, Spoof Detection Schemes, Linkages between Biometrics and Forensic Science, Biometrics in the Government Sector, Biometrics in the Commercial Sector, Biometrics Standards, Biometrics databases	
Text Books & Reference Books (SHOULD Know)	1. Cox I., M. Miller, J. Bloom, J. Fridrich and T Kalker, "Digit Watermarking and Steganography", Second Edition, Morg Kaufmann Publishers, 2008. 2. Jain, Anil K.; Flynn, Patrick; Ross, Arun A. (Eds.), Handbook of Biometrics, Springer, 2008. 3. Borko Furht and Darko Kirovski, —Multimedia Security Handbook‖, 2004 by CRC Press ISBN 9780849327735 4. Stefan Katzenbeisser. Fabien A. P. Petitcolas (Eds). —Information Hiding Techniques for Steganography and Digital Watermarking.‖ Artech House Books **Reference Books:** 1. Chun-Shien Lu, —Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property‖, IDEA GROUP PUBLISHING, 2004

Subject Code	**CE 695**
Subject title	**Cyber-Physical & Self-Organizing Systems**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	31. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 32. One Final Evaluation at the End of the Term **50 Marks** 33. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	CSE, IT, ECE, EE, Robotics, Instrumentation Engg, Industrial Engineering, Modelling & Simulations, Theoretical knowledge of Computer Science and Engineering
Dept	CSE
Course Objective	This course examines a new class of computational systems called Cyber-Physical Systems CPS. Such systems have the potential to provide far-reaching benefits in addressing some of the toughest problems we face as a society, such as: reducing healthcare costs, minimizing traffic congestion, and constructing zero-net energy buildings. Four important features characterize CPS: their ability **monitors the underlying physical environment, reason about the monitored data, control** the physical environment through **actuation**, in a **coordinated**

	manner using a **communication** medium. It can be seen immediately that in CPS, the computational element (cyber) and the environment (physical) are tightly coupled, with one influencing the other. CPS sits at the confluence of several traditional disciplines, such as: embedded systems, real-time systems, sensor networks, control and hybrid systems, and security. It presents many challenging problems and opportunities for research. With guidance from the professor, students will survey recent CPS publications, develop an aptitude. Readings will include papers on CPS applications (e.g., Body Area Networks, smart automobiles, and energy-efficient buildings), issues involved in designing CPS (e.g., monitoring, communication, and control), and how to ensure that the designed systems satisfy certain essential properties (e.g., safety and security).
Syllabus Description	
Unit I: CPS**:** Introduction Main Concepts, Challenges; Background role of Computer Networks, Data, Algorithms **Unit II:** Self-organising Systems, Self-organisation in Natural Systems Inspiring Self-organising Software, **Unit III:** Agents and Multi-Agent Systems Computing trends, Data device proliferation, Confluence of trends **Unit IV:** Technological and economic drivers Self-organisation Mechanisms, Stigmergy , Gossip , Trust and Reputation for Successful Software Self-organisation,Cooperation , Immune Systems, Holonic Multi-Agent Systems Engineering Artificial Self-organising Systems, **Unit V:** Engineering Self-organising Systems, Middleware Infrastructures for Self-organising Pervasive Computing Systems 164 **Unit VI:** Applications of Self-organising Software, Self-organisation in Constraint Problem Solving, Adaptive Trust Management, Security in Artificial Systems	
Text Books & Reference Books (SHOULD Know)	1. Self Organising Software from Natural to artificial Adaptation, Di- MarzoSerugendo, ;Gleizer, M-p; Karageorgos, A (Eds), 2011, XVIII,462P; Hardcover ISBN:978-3642-17347-9 2. —Principles of Cyber-Physical Systems‖ - Rajeev Alur, MIT Press, 2015 3. Research Papers discussed in the classroom discussions

Subject Code	**CE 69B**
Subject title	**Network Forensics**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	34. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 35. One Final Evaluation at the End of the Term **50 Marks** 36. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	CSE, IT, ECE, EE, Robotics, Instrumentation Engg, Industrial Engineering, Modelling & Simulations, Theoretical knowledge of Computer Science and Engineering
Dept	CSE

Course Objective	Network-Administrator & Network-Designer perspectives, develop skill sets to be resourceful in investigating the crimes in the area of Cyber-Security. Enhance analytical capabilities to evaluate a network.
Syllabus Description	
Unit I: Forensics: An Overview, Scope of Network Forensic, Network Forensics Basics 170 Unit II: Network Enabled Operations, Network Controlled Operations, Network Offences, Network Criminalistics Unit III: Basics of host devices on networks: Inter-Network Devices, OS and Networking: A Review Unit IV: Advanced Topics in Computer Network Forensics, Network Forensic Modelling and Principles, Network Forensic Duplication, Network Forensics Analytics, Network File Carving, Network & Cyber Forensics Tools and the Testing of host devices in a network, Mobile Network Device Forensics, IPV6, Network Surveillance and Accountability, Network Attack Traceback and Attribution, Multicast Fingerprinting, Multimedia Forensics Unit V: Intrusion and Online Frauds Detection Unit VI: Peer-2-Peer Networks, Cryptocurrency and Blockchain Unit VII: Network Traffic & Traffic engineering, Network Traffic & Traffic engineering for the Steganography & Steganalysis Unit VIII: Anonymity/Pseudonymity/P2P environments, Network Forensic Challenges in adhoc environments, Network Forensic challenges in IoTs Unit IX: Legal Perspective: Cyber Law, Security and Privacy Policies and Guidelines Unit X: Case Studies, and ethical issues Unit XI: Court Testimony and Report Writing Skills	
Text Books & Reference Books (SHOULD Know)	1. Bruce Middleton, Cyber Crime Investigator's Field Guide, Boca Raton, Florida:Auerbach Publications, 2001, ISBN 0-8493-1192-6. 2. Brian Carrier, File System Forensic Analysis, Addison-Wesley, 2005, ISBN 0-321-26817-2. 3. Chris Prosise and Kevin Mandia, Incident Response: Investigating Computer Crime, Berkeley, California: Osborne/McGraw-Hill, 2001, ISBN 0-07-213182-9. 4. Warren Kruse and Jay Heiser, Computer Forensics: Incident Response Essentials, AdditionWesley, 2002, ISBN 0-201-70719-5. 5. Stephen Northcutt, Mark Cooper, Matt Fearnow, and Karen Frederick, Intrusion Signatures and Analysis, Indianapolis, Indiana: New Riders, 2001, ISBN 0-7357-1063-5.

Subject Code	**CE 602A**
Subject title	**COMPUTATIONAL INTELLIGENCE**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	37. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 38. One Final Evaluation at the End of the Term **50 Marks** 39. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks

Prerequisite	Basic image processing knowledge/computer programming knowledge is required.
Dept	CSE
Course Objective	The course goal is to make students familiar with basic principles of various computational methods of computational intelligence (CI) like nature-inspired methods (neural nets, evolutionary algorithms), fuzzy systems, as well as various probabilistic methods under uncertainty (e.g. Bayesian models) and machine learning methods (e.g. reinforcement learning). After the course the students will be able to conceptually understand the important terms and algorithms of CI, such that they would be able to choose appropriate method(s) for a given task.
Syllabus Description	
Unit I: Introduction to Computational Intelligence: Computational Intelligence Paradigms, Artificial Neural Networks, Evolutionary Computation, Swarm Intelligence, Artificial Immune Systems, Fuzzy Systems, Supervised, unsupervised classification and regression analysis. **Unit II:** Dimensionality Reduction & Feature Selection Methods: Linear Discriminant Analysis and Principal Component Analysis; Data Pre-Processing, Regression, Universal Approximation **Unit III: Evolutionary Computation:** An Overview of Combinatorial Optimization, An Introduction to Genetic Algorithms,Theoretical Foundations of Genetic Algorithms, Genetic Algorithms in Engineering and Optimization, Genetic Algorithms in Natural Evolution, **Unit IV: Swarm Intelligence:** Particle Swarm Optimization, Ant Colony Optimization. **Unit V: Nature Inspired Algorithms for optimization:**Differential Evolution, Simulated Annealing, Multi-objective Optimization, Hybrid Optimization Algorithms	
Text Books & Reference Books (SHOULD Know)	1. Eberhart& Shi, —Computational Intelligence: Concepts to Implementations‖, Morgan Kaufmann, 2007 2. Xin-She Yang, —Nature Inspired Optimization Algorithms‖, Elsevier, 2014 **Reference Books:** 1. AndriesEngelbrecht (2007), —Computational Intelligence: an Introduction‖, Wiley 2. Amit Konar (2005), —Computational Intelligence: Principles, Techniques, and Applications‖, Springer-Verlag Berlin Heidelberg 3. Stuart Russell, Peter Norvig (2009), —Artificial Intelligence – A Modern Approach‖, Pearson Elaine Rich & Kevin Knight (1999), —Artificial Intelligence‖, TMH, 2nd Edition 4. NP Padhy (2010), —Artificial Intelligence & Intelligent System‖, Oxford 5. ZM Zurada (1992), —Introduction to Artificial Neural Systems‖, West Publishing Company 6. Timothy J Ross (2004), —Fuzzy Logic with Engineering Applications‖, John Wiley & Sons Ltd.

Subject Code	**CE 70A**
Subject title	**Formal Specification and Verification of Programs**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	40. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 41. One Final Evaluation at the End of the Term **50 Marks** 42. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks

Prerequisite	
Dept	CSE
Course Objective	To study methods and techniques for stating and proving the correctness statements. Studying Mathematical Logic (Symbolic Logic), Mathematical models for programs. (Programming Language Semantics) and Justification of the verification techniques

Syllabus Description

Reasoning about sequential programs: Programs as (possibly infinite) state transition systems; Specifying program correctness using pre- and post-conditions; partial and total correctness semantics; Hoare logic and its rules for a simple imperative sequential language; weakest pre-condition and strongest post-condition semantics; central importance of invariants in program verification. Brief introduction to lattices and the theory of abstract interpretation; some numerical abstract domains: intervals, difference bound matrices, octagons, polyhedra; computing abstract post-conditions and abstract loop invariants; refining abstractions and counterexample-guided abstraction refinement; Predicate abstraction and boolean programs; converting assertion to a location reachability problem; location reachability using predicate abstraction for simple programs and for programs with (possibly recursive) function calls; Introduction to temporal logics: LTL and CTL; Kripke structures as models of reactive (hardware and software) systems; LTL and CTL model checking algorithms and some applications

Text Books & Reference Books (SHOULD Know)	1. Logic in Computer Science: Modeling and Reasoning about Systems, M. Huth and M. Ryan, Cambridge University Press, 2004 2. Chapter 15, Methods and Logics for Proving Programs by P. Cousot, in Handbook of Theoretical Computer Science, Vol B (Formal Models and Semantics), edited by Jan Van Leeuwen, The MIT Press, 1994 3. Research papers and survey articles to be announced in class

Subject Code	**CE 70B**
Subject title	**Advanced Algorithms**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	43. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 44. One Final Evaluation at the End of the Term **50 Marks** 45. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	
Dept	CSE
Course Objective	

Syllabus Description

Unit I: Basics Data Structures, Abstract Data Types, Dictionaries, Parameters of Algorithms, Growth Functions, Asymptotic Notations & Complexity analysis, Complexity measures. **Unit II: Algorithms** Classic Algorithms, Purpose (S, S, SM, PF, Opti, Prob, Rand), Examples of each, Types of Algorithms, P Type, NP Type, Open Problems, Examples of Algorithms for Internet Search, Web Contents Organization and retrieval **Unit III: Soft-Computing Based Algorithms** Need, Modularity, Sequential, PRAM models, Classic Vs Soft Computing Algorithms, AI enabled Examples of Algorithms for Internet Search, Web Contents Organization and retrieval **Unit IV:Algorithms for AI & Special Applications:** Classic Algorithms, Light-Weight Algorithms & Techniques, Self-Organization & Fault-Tolerance Techniques, Nature Inspired Algorithms **Unit V:Futuristic Trend:** Computations in Cyber Physical Systems CPS, CPS based parallel & distributed Algorithms, Quantum Computing, Concepts of Qubits, Quantum Algorithms, Quantum Search-Space optimization	
Text Books & Reference Books (SHOULD Know)	1. T. H Cormen, C E Leiserson, R L Rivest and C Stein: Introduction to Algorithms, 2nd Edition, Prentice-Hall of India, 2009 (Latest Publication available during training) **Reference Books:** 1. Ellis Horowitz, Sartaj Sahni, S.Rajasekharan: Fundamentals of Computer Algorithms, University Press, 2007. Kenneth A. Berman, Jerome L. Paul: Algorithms, Cengage Learning, 2002. 2. R.Sedgewick, —Algorithms in C++ : Fundamentals, Data Structures, Sorting, Searching, Parts 1-4 (English) 3rd Edition, Pearson. 3. Recommended Research papers during instruction

Subject Code	**CE 700**
Subject title	**Quantum Computing**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	46. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 47. One Final Evaluation at the End of the Term **50 Marks** 48. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	are complex numbers and linear algebra
Dept	CSE
Course Objective	Quantum Computing" is among those terms that are widely discussed but often poorly understood. The reasons of this state of affairs may be numerous, but possibly the most significant among them is that it is a relatively new scientific area, and it's clear interpretations are not yet widely spread. The main obstacle here is the word "quantum", which refers to quantum mechanics - one of the most counter-intuitive ways to describe our world. But fear not! This is not a course on quantum mechanics. We will gently touch it in the beginning and then leave it apart, concentrating on the mathematical model of quantum computer, generously developed for us by physicists. This doesn't mean that the whole course is mathematics either (however there will be enough of it). We will build a

	simple working quantum computer with our bare hands, and we will consider some algorithms, designed for bigger quantum computers which are not yet developed. The course material is designed for those computer scientists, engineers and programmers who believe, that there's something else than just HLL programming, that will move our computing power further into infinity.
Syllabus Description	
1. Unit I: Introduction,Information and Computations, Characteristics of Computational Systems, Computability and Algorithms, Computational Complexity, Quantum Computing parameters and units, The Multiverse Interpretation of Quantum Mechanics **2. Unit II:** Mathematical Model of Quantum Computing, Qubit, Qubit Measurement, Systems with Multiple Qubits, Measuring the Multiple Qubits Systems, Quantum System Evolution & Computations **3. Unit III:** Quantum Computer and Quantum Algorithms,Deutsch's Problem, Quantum Computer Prototype, Suitable Algorithms **4. Unit IV:** Shor's Algorithm, Factoring and the RSA, Factoring and Period Finding, Quantum Fourier Transform **5. Unit V:** Grover's Algorithm. A Quantum Computer Application Boundaries, Grover's Algorithm, Challenges **6. Unit VI:** Quantum environments, Search Spaces, Search Optimisation, Storage Optimisation, Quantum Resources, Future, Challenges	
Text Books & Reference Books (SHOULD Know)	1. Nielsen, Michael A.; Chuang, Isaac L. (June 2012). Quantum Computation and Quantum Information (10th anniversary ed.). Cambridge: Cambridge University Press. ISBN 9780511992773. OCLC 700706156. 2. **References:** Research Papers as discussed in the class room.

Subject Code	**CE 70D**
Subject title	**Computer Network Audit & Forensics**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	1. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 2. One Final Evaluation at the End of the Term **50 Marks** 3. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	Preliminary knowledge Electronic Communications (Graduation Level), Computer Networks (Graduation Level) & IPV4, Networking Devices, Finite State Automata, Socket Programming, Algorithms

Dept	CSE
Course Objective	To meet end-user, Network-Administrator & Network-Designer perspectives, develop skill sets to be resourceful in the area of Cyber-Security. Enhance analytical capabilities to evaluate a Network and Network Enabled Operations to analyze Network Centric Operations

Syllabus Description

Unit I: Basics of host devices on networks: Inter-Network Devices, OS and Networking: A Review, n-tier, peer-to-peer Network architectures
Unit II: Network Protocols, Network Enabled Operations, Network Controlled Operations, Network Offences, Network Criminalities
Unit III: Packet Analysis, Packet Analysis Tools, Network Audit & tools,Network Traffic Engineering, Network Analysis and Analytics
Unit IV: Network Forensics: An Overview, Scope of Network Forensic, Network Forensics Basics
Unit IV: Computer Network Forensic Modelling and Principles, Network Forensic Duplication, Network Forensics Analytics, Network File Carving, Network & Cyber Forensics Tools and the Testing of host devices in a network, Mobile Network Device Forensics, IPV6, Network Surveillance and Accountability
Unit V: Futuristic Networks, Dependable Networks, AI-Enabled Network Environments, Network Virtualization, SDNs, Sensor Networks, IoT, Evolution in Computing Environments like Cloud, Edge, Fog, Ubiquitous, Pervasive

Text Books & Reference Books (SHOULD Know)	1. James Kurose & Keith Ross, Computer Networking: A Top-Down Approach (6th Edition), ISBN-13: 978-0132856201 ISBN-10: 0132856204 2. Packet Analysis Tools, Network Audit Tools and Courseware **Reference books:** 1. Bruce Middleton, Cyber Crime Investigator's Field Guide, Boca Raton, Florida:Auerbach Publications, 2001, ISBN 0-8493-1192-6. 2. Brian Carrier, File System Forensic Analysis, Addison-Wesley, 2005, ISBN 0-321-26817-2. 3. Chris Prosise and Kevin Mandia, Incident Response: Investigating Computer Crime, Berkeley, California: Osborne/McGraw-Hill, 2001, ISBN 0-07-213182-9. 4. Warren Kruse and Jay Heiser, Computer Forensics: Incident Response Essentials, AdditionWesley, 2002, ISBN 0-201-70719-5. 5. Stephen Northcutt, Mark Cooper, Matt Fearnow, and Karen Frederick, Intrusion Signatures and Analysis, Indianapolis, Indiana: New Riders, 2001, ISBN 0-7357-1063-5. 6. Rebecca Gurley Bace, Intrusion Detection, Indianapolis, Indiana: Macmillan Technical, 2000, ISBN 1578701856. 7. Edward Amoroso, Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response, Intrusion.Net Books, 1999, ISBN 0-9666700-7-8. 8. Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, John Wiley & Sons, 2001, ISBN: 0471389226. 9. Alberto Leon-Garcia and Indra Widjaja, Communication Networks: Fundamental Concepts and Key Architectures, First Edition, McGraw-Hill Companies, Inc., 2000, ISBN 0-07-022839-6.

Subject Code	**CE 697**

Subject title	**Biometric Security**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	4. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 5. One Final Evaluation at the End of the Term **50 Marks** 6. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	CSE, IT, ECE, EE, Robotics, Instrumentation Engg, Industrial Engineering, Modelling & Simulations, Theoretical knowledge of Computer Science and Engineering
Dept	CSE
Course Objective	Biometrics has emerged as a specialized field in criminal forensics, public safety surveillance, user authentication and identification. Expansions of biometric modalities are ranged from fingerprint, face and other traits to multimodal biometric traits. Objectives of this course to introduce the students different modality based biometric identification systems, to help them to understand the difference between advanced biometric techniques with respect to traditional authentication mechanisms. Students after learning this course would be able to design and develop biometric systems by utilizing inter-disciplinary knowledge related to fields like Pattern Recognition, Image Processing and Machine Learning etc.

Syllabus Description

1. Introduction: History of Biometrics, Multimodal Biometric Systems, Recent Advances

2. Authentication Technologies, Access Control

3. **Finger Print Biometrics**: Sensors, Dactyloscopy, Types, Algorithms

4. **Handwriting biometrics**: Static and Dynamic Recognition

5. **Iris Biometrics**: Retinal Scanning, Visible and Near Infra red Imaging, Operating Principle, Advantages and Shortcomings

6. **Voice Biometrics**: Verification versus Identification, Text Dependent and Text Independent, Technology, Applications

7. **Face Recognition**: Techniques for Face Acquisition/Recognition, Advantages and Disadvantages, History, Anti-facial recognition

8. **DNA finger printing/ Profiling**: Process, DNA Database, DNA evidence,

9. **Statistical Measures for Biometrics**:

10. **Biometric Devices**: Personal, Handheld, Biometric spoofing, Accuracy

Text Books & Reference Books (SHOULD Know)	1. P. Reid, —Biometrics for Network Security‖, Prentice Hall, 2014. 2. J. Chirrillo and S. Blaul, —Implementing Biometric Security‖, Wiley, 2013. **Reference Book:** 2. AK Jain, —Introduction to Biometrics‖, Springer, 2011. 3. J. Ashborn, —Biometrics: A Complete Guide‖, Springer, 2003

Subject Code	**CE 70E**
Subject title	**Machine Learning in Python**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	7. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 8. One Final Evaluation at the End of the Term **50 Marks** 9. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	basics of probability & statistics is required
Dept	CSE
Course Objective	This course examines the tools and techniques required for learning machine learning algorithms. This course will provide an introduction to the subject and its various applications. Student will learn to implement ML algorithms in python for solving various problems.
Syllabus Description	
UNIT I Basic programming in Python, Introduction: Basic definitions, types of learning, hypothesis space and inductive bias, evaluation, cross-validation. UNIT II Linear regression, Decision trees, overfitting. 178 UNIT III Instance based learning, Feature reduction, Collaborative Filtering based recommendation. UNIT IV Probability and Bayes learning. UNIT V Logistic Regression, Support Vector Machine, Kernel function and Kernel SVM. UNIT VI Neural network: Perceptron, multilayer network, backpropagation, introduction to deep neural networks. UNIT VII Clustering: k-means, Gaussian mixture model.	
Text Books & Reference Books (SHOULD Know)	1. Geron Aurelien, —Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems‖, OReilly, 2017. 2. Jerome H. Friedman, Robert Tibshirani, and Trevor Hastie, —The Elements of Statistical Learning‖, Springer, 2001. 3. Sebastian Raschka, —Python Machine Learning‖, Packt, 1st Edition, 2015

Subject Code	CE 70F
Subject title	**Cloud Computing**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	10. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 11. One Final Evaluation at the End of the Term **50 Marks** 12. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	Basics of computer architecture and Organisation is required.
Dept	CSE
Course Objective	This course will introduce various aspects of cloud computing, including fundamentals, management issues, security challenges and future research trends. This will help students and researchers to use and explore the cloud computing platforms.
Syllabus Description	
UNIT I : Introduction to Cloud Computing, Cloud Computing Architecture UNIT II: Service Management in Cloud Computing, Data Management in Cloud Computing UNIT III : Resource Management in Cloud, Cloud Security UNIT IV : Open Source and Commercial Clouds, Cloud SimulatorWeek 8 : Research trend in Cloud Computing, Fog Computing	
Text Books & Reference Books (SHOULD Know)	1. Cloud Computing from Beginning to End by Ray J Rafaels 2. Cloud Computing: Concepts, Technology & Architecture by Zaigham Mahmood, Ricardo Puttini, Thomas Erl. 3. OpenStack Cloud Computing Cookbook by Kevin Jackson

Subject Code	CE 70H
Subject title	**Cyber Security & Cryptography for Embedded Systems**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	13. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 14. One Final Evaluation at the End of the Term **50 Marks**

	15. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	Basic understanding of Number Theory, Fundamentals of Operating Systems and Knowledge of programming language.
Dept	CSE
Course Objective	Developed the knowledge of security concepts, cyber attacks and technologies to develop secure embedded systems.
Syllabus Description	
Introduction to Security, Introduction to Embedded Security. Vulnerability types, Taxonomy of Attacks, Defense Mechanisms, Mathematics of Cryptography, Basics of symmetric versus asymmetric key encryption. Early ciphers - Substitution, permutation and product ciphers. Block versus stream ciphers. Basics of entropy and perfect secrecy, Mathematical foundations of the 180 discrete logarithm problem, Diffie-Hellman Key Exchange, Mathematical foundations of RSA, Encryption using Elliptic curve The cryptographic hash – properties, Data Integrity, The cryptographic hash - construction, the Birthday paradox, Message Authentication, digital signature. Side Channels attacks on Embedded Systems, Embedded Cryptography, A5 Encryption for GSM, Hardware based Security. Transport layer security (TLS/SSL), FPGA based encryption and Decryption	
Text Books & Reference Books (SHOULD Know)	1. Hardware Security: Design, Threats and Safeguards‖ by Debdeep Mukhopadhyay and Rajat Subhra Chakrabarty, CRC Press,2015. 2. Cryptography & Network Security‖ by William Stallings4th Edition, 2006, Pearson Education Asia. 3. Cryptography and Network Security‖ by Behrouz A. Forouzan, Mc Graw Hill. 4. Cryptography & Network Security‖ by Kahate A, Tata Mc Graw Hill, 2004. 5. Morrie Gasser: Building a Secure Computer System 6. Michael Ligh, Steven Adair, Malware Analysts‘s cookbook, Wiley publishing

Subject Code	**CE 682**
Subject title	**Secure Software Engineering**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	16. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 17. One Final Evaluation at the End of the Term **50 Marks** 18. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	C programming and debugging. Basic concept of Operating Systems.
Dept	CSE
Course Objective	Students will acquire an understanding of the fundamental concepts for developing secure systems □ Introduce security requirements, Security Policies, Architecture of Secure Software and Boot Integrity □ Attacker models

	Fundamentals of data protection and privacy
Syllabus Description	
Fundamentals of Software Engineering: Requirements Engineering, Design Concepts, Software Testing Fundamentals. Confinement, Boot integrity, Architectural approaches to building secure Software, Dynamic Root of trust for Measurement, Run- time enforcement of Security Policies, Software only root of trust (SWORT), Usable and Secure Password, Security Protocols and Verification, Static Analysis of software, Combining static and dynamic analysis, Control Flow Integrity, Language based Approaches to building Secure Software.VAPT analysis, secure coding techniques,	
Text Books & Reference Books (SHOULD Know)	1. Software Engineering - Roger S Pressman - 5th edition. 2. An Integrated Approach to Software Engineering, PankajJalote Third Edition, NarosaPublishing House 3. The security Development Lifecycle, by Michael Howard and Steve Lipner 4. Security in Computing, By Charles P. Pfleeger , Shari Lawrence Pfleeger, Publisher: PrenticeHall Print ISBN-10: 0-13-239077-9 5. Threat Modeling by Frank Swiderski, Window Snyder, Microsoft Press, ISBN-10:0735619913 6. Research Paper and Articles in Journals and Conference Proceedings.

Subject Code	**AM625**
Subject title	**Digital Image Processing**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	19. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 20. One Final Evaluation at the End of the Term **50 Marks** 21. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	
Dept	CSE
Course Objective	
Syllabus Description	
Digital Image Fundamentals: Introduction – Origin –Steps in Digital Image Processing –Components; Elements of Visual Perception – Light and Electromagnetic Spectrum – ImageSensing and Acquisition – Image Sampling and Quantization – Relationships between pixels. 204 **Image Enhancement:** Spatial Domain: Gray level transformations – Histogram processing –Basics of Spatial Filtering–Smoothing and Sharpening Spatial Filtering – Frequency Domain:Introduction to Fourier Transform – Smoothing and Sharpening frequency domain filters – Ideal,Butterworth and Gaussian filters.	

Image Restoration: Noise models – Mean filters – Order Statistics – Adaptive filters – Band reject – Band pass – Notch – Optimum notch filtering – Inverse Filtering – Constrained Least Square Filtering – Wiener filtering. **Morphological image processing:** Dilation, Erosion, Opening, Closing, Applications to; Boundary extraction, Region filling, Extraction of connected components. **Image Compression:** Fundamentals – Image Compression models – Error Free Compression –Variable Length Coding –Bit – Plane Coding – Lossless Predictive Coding – Lossy Compression– Lossy Predictive Coding –Wavelet Coding – Compression Standards – JPEG2000. **Image Segmentation and Representation:** Segmentation – Detection of Discontinuities – EdgeLinking and Boundary detection – Region based segmentation; Representation – Boundary descriptors – Simple Descriptors – Shape numbers –Regional descriptors – Simple and Topological Descriptors – Introduction to Image Processing Toolbox – Practice of Image Processing Toolbox – Case studies–Various Image Processing Techniques. **Object recognition:** Decision-theoretic methods.	
Text Books & Reference Books (SHOULD Know)	1. Digital Image Processing, 3rd Ed., 2007, R. C. Gonzalez, Richard E. Woods, Prentice Hall. 2. Digital Image Processing Using MATLAB, 2nd Ed., 2009, R. C. Gonzalez, Richard E.Woods, Steven L. Eddins, Gatesmark Publishing. 3. Digital Picture Processing, 2nd Ed., 1982, A. Rosenfeld, A. C. Kak, Academic Press. 4. Fundamentals of Digital Image Processing, 1st Ed., 1989, A.K. Jain, Prentice Hall of India. 5. Pattern Classification and Scene Analysis, 1973, R. O. Duda, P. E. Hart, John Wiley. 6. Pattern Recognition, Applications to Large Data-Set Problems, 1984, Sing-Tze Bow, Marcel Dekker

Subject Code	**EE 613**
Subject title	**ELECTRONIC WARFARE**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	22. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 23. One Final Evaluation at the End of the Term **50 Marks** 24. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	
Dept	CSE
Course Objective	
Syllabus Description	

UNIT-I: INTRODUCTION TO ELECTRONIC WARFARE: Electronic Defence, Electronic Combat (ESM-ECM-ECCM), Radar Basics (Radar Technology Evolution, Radar Range Equation, RCS Reduction, Counter-Low Observable), SIGNIT, Intercept System Characteristics and Functions, Frequency Coverage, Analysis Bandwidth, Wideband Radar Signal Trends, Dynamic Range, Dynamic Range Requirements, Sensitivity, Noise Figure Measurement, Y-Factor Measurement, Some Sensitivity Measures, Output SNR and Receiver Applications, Threshold Detection, Sensitivity and the Received Pulse Density, The Ultimate Limits to ELINT Parameter Measurements, Probability of Intercept. **UNIT-II: ELECTRONIC SUPPORT MEASURES:** Typical ESM Systems, ESM Sensitivity, ESM Receivers - Crystal Video Receiver, IFM Receiver, Super heterodyne Receiver, Channelized Receiver, Bragg Cell Receiver, Compressive Receiver, Digital Receivers. DOA/AOA Measurement Emitter Location - The Role of Emitter Location ,Emitter Location Geometry ,Emitter Location Accuracy, Amplitude-Based Emitter Location, Interferometer Direction Finding, Interferometric DF Implementation, Direction Finding Using the Doppler Principle, Time of Arrival Emitter Location. **UNIT-III: ELECTRONIC COUNTER MEASURES:** Principals of Electronic Attack (EA), Jamming-to-Signal Ratio , Jamming Types(Burn-Through, Cover Jamming ,Range Deceptive Jamming, Inverse Gain Jamming, Repeater Jamming Equations, Noise Jamming vs. Deception, Repeater vs. Transponder, Side lobe Jamming vs. Main lobe Jamming, Stand-Off Jamming, Escort Jamming, Self Protection Jamming, ECM techniques, On-Board ECM Systems, Off-Board ECM Systems, Infrared Countermeasures (IRCM), Off-Board ECM Systems, Communications Countermeasures (COM-ECM), Electro-Optic Counter Measure (Eocm) Systems¸ Airborne Tactical Jamming System, Shipboard Self-Defense System, EA/Susceptibility against Weapon Systems. **UNIT-IV: ELECTRONIC COUNTER-COUNTERMEASURES:** Search Radar Counter-Countermeasures, Tracking Radar Counter-Countermeasures, Infrared Counter-Countermeasures, Communications Counter-Countermeasures. 337 **UNIT-V: NEW ELECTRONIC DEFENSE TECHNIQUES:** New Electronic Defense Techniques and Technologies trend, Shared Apertures/MRFS, Anti Anti-Radiation Missile Techniques, Anti-Stealth Techniques, RF Direct Energy Weapons, Design and Evaluation Criteria: Design Criteria, Evaluation Criteria for the Choice of a System, Operational Effectiveness, Electronic Defense and Conventional Defense, Electronic Warfare Digitization.	
Text Books & Reference Books (SHOULD Know)	1. EW101: A First Course in Electronic Warfare, David Adamy, Artech House 2. EW102: A Second Course in Electronic Warfare, David Adamy, Artech House 3. Introduction to Electronic Defence Systems, Second Edition, Artech House by Filippo Neri 4. Introduction to Electronic Warfare 1984, Schleher Dc, Artech House 5. Microwave Receiver with EW applications, 1986, James Bao& Yen Tsui, Wiley and Sons. **REFERENCE BOOKS:** 1. Electronic Warfare in the Information Age, 1999,D. Curtis Schleher, Artech House, Boston, London 2. Radar hand book, 1972/1990, Skolnik MI, Mc Graw Hill. 3. Fundamentals of Electronic Warfare, Artech House by Sergei A. Vakin

Subject Code	**TM609**
Subject title	**SYSTEMS ENGINEERING**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	25. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 26. One Final Evaluation at the End of the Term **50 Marks** 27. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	

Dept	CSE
Course Objective	

Syllabus Description

Unit I : SYSTEMS ENGINEERING AND THE WORLD OF MODERN SYSTEMS

- What Is Systems Engineering?
- Origins of Systems Engineering
- The Power of Systems Engineering
- Examples of Systems Requiring Systems Engineering

Unit 2 : STRUCTURE OF COMPLEX SYSTEMS

- System Building Blocks and Interfaces
- Hierarchy of Complex Systems
- System Building Blocks
- The System Environment
- Interfaces and Interactions
- Complexity in Modern Systems
- Examples of Complex Systems

Unit 3: THE SYSTEM DEVELOPMENT PROCESS

- Systems Engineering through the System Life Cycle
- System Life Cycle
- Evolutionary Characteristics of the Development Process
- The Systems Engineering Method
- Testing throughout System Development
- Development process examples

Unit 4: SYSTEMS ENGINEERING MANAGEMENT

- Managing System Development and Risks
- WBS
- SEMP
- Risk Management

Text Books & Reference Books (SHOULD Know)	1. B.Dennis M.Buede, The Engineering Design of Systems: Models and Methods, John Wiley& Sons,2011 306 2. A.Kossiakoff, W.N.Sweet,S.J.Seymour & S.M.Biemer,Systems Engineering: Principles and Practice,Wiley,2011 3. D.J.E.Kasser,A Framework for Understanding Systems Engineering, Book/Surge Publishing,2007 **References Books:** 1. George,A. Hazelrigg, Systems Engineering: An Approach to Information-Based Design, Prentice Hall NJ, 1996. 2. Benjamin, A., Blanchard, and Walter,J. Fabrycky, Systems Engineering and Analysis, 3rd Ed., Prentice Hall International Series, Industrial & Systems Engg., 1998 3. B.S.Blanchard, Systems Engineering Management,Wiley,1998

Subject Code	CE 69F
Subject title	**Theory of Computation**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	28. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 29. One Final Evaluation at the End of the Term **50 Marks** 30. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	CSE, IT, ECE, EE, Robotics, Instrumentation Engg, Industrial Engineering, Modelling & Simulations, Theoretical knowledge of Computer Science and Engineering
Dept	CSE
Course Objective	This course examines a new class of computational systems called Cyber-Physical Systems CPS. Such systems have the potential to provide far-reaching benefits in addressing some of the toughest problems we face as a society, such as: reducing healthcare costs, minimizing traffic congestion, and constructing zero-net energy buildings. Four important features characterize CPS: their ability **monitors the underlying physical environment, reason about the monitored data, control** the physical environment through **actuation**, in a **coordinated** manner using a **communication** medium. It can be seen immediately that in CPS, the computational element (cyber) and the environment (physical) are tightly coupled, with one influencing the other. CPS sits at the confluence of several traditional disciplines, such as: embedded systems, real-time systems, sensor networks, control and hybrid systems, and security. It presents many challenging problems and opportunities for research. With guidance from the professor, students will survey recent CPS publications, develop an aptitude. Readings will include papers on CPS applications (e.g., Body Area Networks, smart automobiles, and energy-efficient buildings), issues involved in designing CPS (e.g., monitoring, communication, and control), and how to ensure that the designed systems satisfy certain essential properties (e.g., safety and security).

Syllabus Description

1.**Introduction**: Motivation, , Terminology, History

2. **Computers and Science of Computing:** Computability, Undecidability, Intractability, and Intelligence

3. **Automata**: Construction, Finite Automata, Limitations of Finite Automata

4. **Non-Deterministic Finite Automata**, Moore Machine, Mealy Machine

5. **Regular Languages and Expressions**: Equivalence, Regular expressions in practice

6. **Grammars**: Parsing and Derivation, Grammar for regular languages, Converting Regular grammar to Automata

7. **Nature of Regular Languages:** Closure properties, Peigeonhole principle, Pumping Lemma, Adversarial Game

8. **Context Free Languages and Grammars**: Context Free Behaviour, CFGs, Ambiguity, Chomsky Normal Form, Simple, Linear and other grammars

9. **Pushdown Automata**: Stack Behviour, Constructing PDAs, CFGs to PDAs, CFL-CFG-PDA Triad

10. **Nature of Context Free Languages**: Closure properties

11. **Turing Machines**: Construction, Definition, Complex Turing Machines, Church Turing Thesis, Universal Turing Machines 12. **The Chomsky Hierarchy**: Languages, Grammars and Machines, Recursive Languages, Idea of Context 13. **Computability and Undecidability**: Halting Problem, P = NP?	
Text Books & Reference Books (SHOULD Know)	1. K. Mahesh, —Theory of Computation: A problem solving approach‖, Wiley publishers. 2015 2. Hopcroft, Motwani & Ullman, —Introduction to Automata Theory, Languages and Computation‖, 3rd Edition, Pearson, 2007. **Reference Book:** 1. M. Sipser, —Introduction to Theory of Computation‖, 3rd Edition, Wordsworth Publishing, 2012.

Subject Code	**AM 628**
Subject title	**Computational Number Theory and Cryptography**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	31. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 32. One Final Evaluation at the End of the Term **50 Marks** 33. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	CSE, IT, ECE, EE, Robotics, Instrumentation Engg, Industrial Engineering, Modelling & Simulations, Theoretical knowledge of Computer Science and Engineering
Dept	CSE
Course Objective	Attacks, Services and Mechanisms, Security attacks, Security services, A Model for Internetwork security. Classical Techniques: Conventional Encryption model, Steganography, Conventional Encryption Principles, Conventional encryption algorithms, cipher block modes of operation, location of encryption devices
Syllabus Description	
Divisibility: Representations of Integers, Computer Operations with Integers, Complexity of Integer Operations, Divisibility, Prime Numbers, The Fundamental Theorem of Arithmetic, Sieve 227 of Eratosthenes, The Distribution of Primes, Greatest Common Divisor, Euclidean Algorithm, Mersenne Numbers, Fermat Numbers, Perfect numbers **Congruence**: Congruences, Congruence Applications, Linear Congruences, The Chinese Remainder Theorem, Theorems of Fermat and Euler- Fermat, Wilson's Theorem, Pseudo Primes, Carmichael Numbers, The Euler Phi-Function, The Sum and Number of Divisors, Quadratic Residue, Quadratic Reciprocity. **Factorization and Primality Testing**: Complexity of Number Theoretic Algorithms, Fermat's Factorization, Kraitchik's Improvement, Pollard Rho Algorithm, Legendre and Jacobi Symbols, Computing Legendre symbols, Primitive Roots, Pseudo Primality Testing, Miller-Rabin Algorithm, Quadratic Reciprocity Law **Finite fields**: Groups, Fields, Finite Fields, Arithmetic in Finite Field, Finding Multiplicative Inverses in finite fields, Binary Fields and their application in Cryptosystems, Primitive roots. **Cryptography**: Introduction to Cryptosystems, Classical Ciphers, Cryptanalysis of Classical ciphers, LFSR based stream ciphers. Shannon's Theory, Public Key Cryptography, RSA Cryptosystem, Diffie-Helman Key Exchange, Rabin Cryptosystem, Knapsack Ciphers, Digital Signature, Secret Sharing, ElGamal Cryptosystem, Elliptic Curve Cryptography.	

Elliptic Curve Cryptography: Introduction to Elliptic Curves, Geometry of Elliptic curves over Reals, Weierstrass Normal form, Point at infinity, Elliptic Curves over Finite fields, Group structure, Discrete Log problem for Elliptic curves, Factorization using Elliptic Curve, Advantage of Elliptic Curve Cryptography over other Public Key Cryptosystems.	
Text Books & Reference Books (SHOULD Know)	1.N. Koblitz, A Course in Number Theory and Cryptography, Springer 2006. 2. I. Niven, H.S. Zuckerman, H.L. Montgomery, An Introduction to theory of numbers, John Wiley & Sons, Inc 2006. 3. L. C. Washington, Elliptic curves: number theory and cryptography, Chapman & Hall/CRC, 2003. 4. J. Silverman and J. Tate, Rational Points on Elliptic Curves, Springer-Verlag, 2005. 5. D. Hankerson, A. Menezes and S. Vanstone, Guide to elliptic curve cryptography, SpringerVerlag, 2004. 6. J. Pipher, J. Hoffstein and J. H. Silverman , An Introduction to Mathematical Cryptography, Springer-Verlag, 2008. 7. G.A. Jones and J.M. Jones, Elementary Number Theory, Springer-Verlag, 1998. 8. R.A. Mollin, An Introduction to Cryptography, Chapman & Hall, 2001. 228 9. Song Y. Yan: Number Theory for Computing, Springer-Verlag, Second Edition,2002. 10. T. H. Cormen, C. E. Leiserson, and R. L. Rivest: Introduction to Algorithms, Second Edition, Prentice Hall of India, 1994. 11. K. Rosen: Elementary Theory of Numbers, Fifth Edition, Addison Wesley, 2004

CE699 Internet of Things

Syllabus:

Unit I Introduction to Internet of Things, Definition and Characteristics of IoT, Physical Design of IoT, IoT Protocols, IoT communication models, IoT Communication APIs

Unit II IoTenablingTechnologies, Wireless Sensor Networks, Cloud Computing, Big data analytics, Communication protocols, Embedded Systems, IoT Levels and Deployment Templates, Domain Specific IoTs: Home, City, Environment, Energy, Retail, Logistics, Agriculture, Industry, health and Lifestyle

Unit III 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 IV IoT physical end devices & end points, IoT Physical Servers & Cloud offerings,Software environments, NEO, Security

Text /Reference Books:

1. "Internet of Things: A Hands-on Approach", by ArshdeepBahga and Vijay Madisetti (Universities Press), 2014
2. "The Internet of Things: Enabling Technologies, Platforms, and Use Cases", by PethuruRaj and Anupama C. Raman (CRC Press)
3. “Designing the internet of things”, McEwen, Adrian, and Hakim Cassimally. John Wiley& Sons, 2013.
4. Research Papers discussed in the classroom discussions.

CE691 SECURE WIRELESS SENSOR NETWORKS

Background: Wireless Sensor networks (WSN) is an emerging technology and have great potential to be employed in critical situations like battlefields and commercial applications such as building, traffic surveillance, habitat monitoring and smart homes and many more scenarios. One of the major challenges wireless sensor networks face today is security. While the deployment of sensor nodes in an unattended environment makes the networks vulnerable to a variety of potential attacks, the inherent power and memory limitations of sensor nodes makes conventional security solutions unfeasible. The sensing technology combined with processing power and wireless communication makes it profitable for being exploited in great quantity in future. The wireless communication technology also acquires various types of security threats.

Objective: To meet End-User, Network-Administrator and Network-Designer perspectives

Prerequisite: Computer Networks Fundamentals, Programming,

Syllabus:

Unit I: Introduction, WSN Resources & constraints, Relevance to IoTs, Relevance to Cyber-Physical Systems, Relevance to Network Centric Operations, Relevance to Data Stream Management Systems, Relevance to the increasing demand of high performance computations, SCADA, battle sensor.

Unit II: WSN Network Architecture, MAC Layer protocols, Naming and Addressing, Synchronization, Location & positioning, Topology control, Connected Dominating Sets, Routing Protocols, Data-Centric & Content-based networking, Data-Centric querying, WSNs versus IoTs

Unit III: Vulnerabilities, threats, attacks & safeguards in WSN, key distribution methods & protocols, multi-party computations inclusion, RF-Id communications, open source hardware concept, Security goals for WSNs, Attacks on WSNs: Passive & Active Attacks, Security Mechanisms, Security Models for WSNs, Challenges in WSNs: with respect to wireless medium, resource scarcity, ad-hoc deployments, hostile environments, immense scale, etc. Application oriented: Secure Wireless Networks.

Text Book:

1. FUNDAMENTALS OF WIRELESS SENSOR NETWORKS: THEORY AND PRACTICE, Authors: Waltenegus Dargie, Technical University of Dresden, Germany, Christian Poellabauer, University of Notre Dame, USA, Wiley, First Edition, 2010

Research Paper References:

1. Ian F. Akykildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, —A Survey on Sensor Networks‖, IEEE Communication Magazine, year 2002.
2. Culler, D. E and Hong, W., —Wireless Sensor Networks‖, Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.
3. Adrian Perrig, John Stankovic, David Wagner, —Security in Wireless Sensor Networks‖ Communications of the ACM, Page53-57, 2004
4. Chris Karlof, David Wagner, —Secure Routing in Wireless Sensor Networks: Attacks and

Countermeasures‖, AdHoc Networks (elsevier), Page: 299-302, year 2003
5. Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, —Security in Wireless Sensor Networks: Issues and Challenges‖, International conference on Advanced Computing Technologies, Page1043-1045, year 2006
6. John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, —Wireless Sensor Network Security: A Survey‖, Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10-15, year 2006
7. Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong, —Security in wireless sensor networks: issues and challenges‖ Advanced Communication Technology (ICACT), Page(s):6, year 2006
8. Tahir Naeem, Kok-Keong Loo, Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks, International Journal of Digital Content Technology and its Applications, Page 89-90 Volume 3, Number 1, year 2009
9. Undercoffer, J., Avancha, S., Joshi, A. and Pinkston, J. —Security for sensor networks‖. In Proceedings of the CADIP Research Symposium, University of Maryland, Baltimore County, USA, year 2002 http://www.cs.sfu.ca/~angiez/personal/paper/sensor-ids.pdf
10. Zia, T.; Zomaya, A., —Security Issues in Wireless Sensor Networks‖, Systems and Networks Communications (ICSNC) Page(s):40 – 40, year 2006
11. Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou, Sensor Network Security: A Survey, IEEE Communications Surveys & Tutorials, vol. 11, no. 2,page(s): 52-62, year 2009
12. D. Djenouri, L. Khelladi, and N. Badache, —A Survey of Security Issues in Mobile ad hoc and Sensor Networks,‖ IEEE Commun. Surveys Tutorials, vol. 7, pp. 2–28, year 2005.
13. S. Schmidt, H. Krahn, S. Fischer, and D. Watjen, —A Security Architecture for Mobile Wireless Sensor Networks,‖ in Proc. 1st European Workshop Security Ad-Hoc Sensor Networks (ESAS), 2004.
14. Y. Wang, G. Attebury, and B. Ramamurthy, —A Survey of Security Issues in Wireless Sensor Networks,‖ IEEE Commun. Surveys Tutorials, vol. 8, pp. 2–23, year 2006.
15. Yun Zhou, Yuguang Fang, Yanchao Zhang, Securing Wireless Sensor Networks: A Survey, IEEE Communications Surveys & Tutorials, year 2008
16. Xiuli Ren, Security Methods for Wireless Sensor Networks, Proceedings of the 2006 IEEE International Conference on Mechatronics and Automation , Page: 1925 ,year 2006
17. R.Roman, J. Zhou, and J. Lopez, —On the security of wireless sensor networks,‖ in International Conference on Computational Science and Its Applications – ICCSA 2005, May 9-12 2005, vol. 3482 of Lecture Notes in Computer Science, (Singapore), pp. 681– 690, Springer Verlag, Heidelberg, D-69121, Germany, 2005.
18. N. Sastry and D. Wagner, —Security considerations for ieee 802.15.4 networks,‖ in Proceedings of the 2004 ACM workshop on Wireless security, pp. 32–42, Philadelphia, PA, USA: ACM Press, 2004.
19. WSN Security Models: Refer 4 papers: Paper 1: Wireless sensor network security model using zero knowledge protocol, ICC 2011; Paper 2. An energy efficient link-layer security protocol for wireless sensor networks, EIT 2007; Paper 3. Toward resilient security in wireless sensor networks, MobiHoc 2005; Paper 4. TinySec: a link layer security architecture for wireless sensor networks, SenSys 2004.

Tutorials:

a. Routing techniques: Overview of Proactive and reactive routing protocols, significance of *a hop* in adhoc networks
b. Flooding, Gossiping, Zonal Routing Protocols ZRP, Hybrid Routing, TTL significance with respect to routing protocols
c. Impact of hardware and software on Battery Performances/Utilisation
d. IEEE 802.15.4: A study, Features, Types of Devices FFD (PAN coordinators, Coordinators), RFDs

Reduced Function Devices, Network Setup process & parameters in Consideration, Programming Strategies to suit the standards, MAC and PHY structure

e. Demo 1: Controlling DIOs. Demonstrate the usage of DIO using LEDs. Learning how to handle data sampling period.
f. Demo 2. Reading data from a single IoT device. Interpretation of data.
g. Demo 3: Create a broadcast wireless network and capture the traffic generated by the participating nodes.
h. Demo 4. Creating a multi-hop network using MBR routing.
i. Understanding MBR & LBR (MAC Based Routing and LBR Level-Based Routing)
j. Understanding exiting API, Libraries & its association with pre-existing demonstration codes.

M.Tech. Computer Science & Engineering (Artificial Intelligence)

Introduction

Artificial Intelligence (AI) based systems have become an essential factor in economic, social development and almost in every facet of our daily lives. AI, deep learning and machine learning are becoming thrust areas and prominent field of study. Professionals who are trained in this field are highly regarded and contribute to strengthening the social, political and financial fabric of modern society.

Program Objectives The MTech (AI) programme aims at developing Human Resources in the field of AI with athrust on defence related problems. The present programme is conceived to understand, assimilate & use the advanced technologies to design and develop AI based systems to solve society/ defence problems. Advanced technologies in the areas of deep learning, robotics, machine learning, computer vision, video surveillance, text analytics, speech

analytics are the topics/components of this curriculum.

Eligibility

Minimum CPI of 6.5 or 60% of marks or first class in qualifying degree. Bachelor degree in Engineering/Technology or Equivalent in CS/IT/ECE/ETC/EE or in relevant Disciplines and a valid GATEScore.

Program Outcome To generate highly skilled manpower, to research, design, develop and test reliable AI based systems to solve critical problems in various sectors. After completing this course, students are expected to understand and practice the essential concepts related to AI.

Organization The Programme curriculum has been designed considering the cyber security requirements of Industry and Defence research and development. It is designed and reviewed by panel of experts chosen from various DRDO labs and leading academic institutions. Each Course of 4 credits is delivered by Course experts through the duration of 16 weeks approximately. It consists of 3 hrs of class room interaction and 2 hrs of lab sessions per week. The evaluations follow continuous assessment process that includes – 3 monthly evaluation exams (10 Marks each), internal assessment (20 Marks) and final examination (50 Marks). The lab focuses on practical exposure to the cyber security tools and techniques in form of mini projects and lab assignments. The 3rdand 4th semesters have a major component of MTech project dissertation, where the students work under close supervision and guidance of their project guide. The students present their work at the end of 3rd and 4th semester. The MTech thesis is submitted and evaluated by the panel of expert examiners at the end of 4th semester.

Program Educational Objectives (PEOs)

PEO1 The M.Tech. Computer Science and Engineering aims at developing skilled Human Resources in the field of Cyber Security and Artificial Intelligence by providing two different specializations, catering the emerging multidisciplinary problem-solving needs of defense, civil and DRDO sectors.

PEO2 The M.Tech. in Cyber Security(CS) programme aims at developing skilled Human Resources in the field of Cyber Security with a thrust on solving defence and society related problems. The present programme is conceived to understand, assimilate & use the advanced technologies such as Network security, Cryptography, Ethical Hacking, Digital Forensic, Malware Analysis, Information Security Management and Trusted Computing techniques. After completing this course, students are expected to understand and practice the essential CS concepts along with developing secure systems.

PEO3 The M.Tech. Computer Science and Engineering with specialization in Artificial Intelligence programme aims at developing skilled Human Resources in the field of AI with a thrust on solving defence and society related problems. The present programme is conceived to understand, assimilate & apply the advanced technologies such as deep learning, robotics, machine learning, computer vision, video surveillance, text analytics, speech analytics etc. After completing this course, students are expected to understand and practice the essential AI concepts along with developing AI based systems to solve society/defence related problems, carry out research and innovation.

Program Outcomes (PO)

PO1 The M.Tech. Computer Science and Engineering aims at developing an ability in students to independently carry out research /investigation and development work to solve practical problems

PO2 The M.Tech. Computer Science and Engineering aims at developing an ability in students to write and present a substantial technical report/document

PO3 The M.Tech. Computer Science and Engineering students should be able to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program

Program Specific Outcomes (PSO)

PSO1 The M.Tech. Computer Science and Engineering aims at developing skilled knowledgeable Human task force in the field of Cyber Security, catering the needs of defence, social and DRDO requirements

PSO2 The M.Tech. Computer Science and Engineering aims at developing skilled knowledgeable Human task force in the field of Artificial Intelligence, catering the needs of defence, social and DRDO requirements.

Semester I

Sr. No.	Course Code	Course	Contact Hours / Week		Credits
			L	T/P	
1	CE-601	Responsible Artificial Intelligence	3	1	4
3	CE-602	Intelligent Algorithms	3	1	4
4	CE-603	Deep Neural Networks	3	1	4
5	CE-604	Practical Machine Learning	3	1	4
6	CE-605	Mathematics for Machine Learning	3	1	4

7	AM-607	Mathematics for Engineers	3	1	4
8	PGC-601	Research Methodology and IPR	2	0	2
		Total	**20**	**6**	**26**

Tech

Semester II

Sr. No.	**Course Code**	**Course**	**Contact Hours / Week**		**Credits**
			L	T/P	
1	CE-611	Computer Vision	3	1	4
2	CE- 612	Adversarial and Generative AI	3	1	4
3		Elective I (from Department)	3	1	4
4		Elective II (from Department)	3	1	4
5		Elective III	3	1	4
6		Elective IV	3	1	4
7	PGC-602	Audit 1 and 2	2	0	0
		Total	**20**	**6**	**26**

SEMESTER III

Sl. No.	**Course Code**	**Course**	**Contact Hours /week**		**Credits**
			L	**T/P**	
1	CE-651	M.Tech. Dissertation Phase-I	28		14
		Total	**28**		**14**

SEMESTER IV

Sl. No.	Course Code	Course	Contact Hours /week		Credits
			L	T/P	
1	CE-652	M.Tech. Dissertation Phase-II	28		14
		Total	**28**		**14**

List of Audit Courses (Applicable for Sem - II):

Sr.No.	Course Code	Course
9.	**PGC-602**	English for Research Paper Writing
10.		Disaster Management
11.		Sanskrit for Technical Knowledge
12.		Value Education
13.		Constitution of India
14.		Pedagogy Studies
15.		Stress Management by Yoga
16.		Personality Development through Life Enlightenment Skills

List of Open Electives Semester-II

Sr. No.	Course Code	Course
1.	CE- 613	Large Language Models
2.	CE-695A	Cyber Physical Systems
3.	CE-630	Virtual Reality
4.	CE-665A	Security Standards and Penetration Testing
5.	CS-611	Digital Forensics
6.	CS-612	Reverse Engineering & Malware Analysis
7.	CE-70G	Blockchain Technology
8.	CE-66A	Algorithmic Cryptanalysis
9.	CE-699	Internet of Things
10	CE-633	Pattern Recognition

11	CE-691	Secure Wireless Sensor Networks
12	CE-606A	Software Engineering & System Modelling
13	CE-694	Big Data Analysis and Algorithms
14	• Open Electives	

- The electives and other Core Courses offered in the 2nd semester by the other departments may be opted by the students on consultation with the course OIC.

SEMESTER I CORE COURSES

Subject Code	**CE-601**
Subject title	**Responsible Artificial Intelligence**
Credit	**04**
Type of Subject	-Core (MTech in CSE) -Professional Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	4. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 5. One Final Evaluation at the End of the Term **50 Marks** 6. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	Statistics, any one Programming Language, Knowledge of the following will help: Data Storage and Retrieval Techniques, SQL, Algorithms. [These will be introduced, time-to-time during instructions as preliminaries]
Dept	CSE,SoCEMS
Course Objectives	The rise of Artificial Intelligence (AI) has brought about unprecedented advancements across various sectors, from healthcare to finance to everyday consumer technology. This subject dwells in concepts of database, data-in-transit, data-at-storage and use of data for decision making in decision support systems. The advancements come with critical challenges. The fairness of AI systems is the need of the hour to study & be able to evaluate. It is essential to ensure that these technologies benefit all individuals and groups without perpetuating or exacerbating existing biases and inequalities
Course Outcomes	1. Student will be able to identify and quantify biases using statistical/ mathematical techniques. 2. Student will be able to evaluate and implement models to incorporate desired features of fairness. 3. Student will be able to design and implement to incorporate fairness constraints 4. Student will be able to create interpretable models and generate explanations for AI decisions.

CO

	PO1	PO2	PO3	PSO1	PSO2
CO1	Y	Y		Y	Y
CO2	Y	Y		Y	Y
CO3		Y	Y	Y	Y
CO4		Y	Y	Y	Y

Syllabus Description

Basics & Preliminaries	**Details**	**Books & References**	**Duration**
Unit-1- AI Fundamentals and Introduction to Responsible AI	Definition and scope of Artificial Intelligence, key concepts and terminology, overview of AI sub-fields (machine learning, natural language processing, LLMs), status of the technology, applications of AI across a range of domains and sectors, need of ethical and responsible AI, examples of AI/ML systems going wrong.	Inspired from MSt in AI Ethics and Society by University of Cambridge, Course in Responsible Artificial Intelligence (CourseCode- DS5604) by IIT Palakkad. Covered by [1] & [2].	12
Unit-2 Principles of Responsible AI	Principles of Responsible AI: inclusive growth, sustainable development and well-being; human-centred values and fairness; transparency and explainability; robustness, security and safety; accountability. Problems with ML models - bias, robustness, generalization to OOD samples, adversarial examples, data protection; problems with generative models: hallucination, factual correctness, prompt injection, data leakage, deep fakes, copyright infringement, etc. Near- and long-term challenges of AI (misuse, misgeneralisation, rogue AGI), AI risks for Gen models, Adversarial attacks – text, images, NLP; examples will be drawn from various incidents	Inspired from Certificate Program on Responsible AI-Tour by IIT Madras, Certification Program on Responsible & Safe AI systems by IIIT Hyderabad and IIT Madras and the OECD AI Principles. Covered by [1], [2], [7] & [9].	12
Unit-3 Assessing AI Fairness and Robustness	AI Fairness - sources of bias, exploratory data analysis, limitation of datasets; preprocessing, in-processing and post-processing to remove bias; group fairness and individual fairness, counterfactual fairness; fairness metrics, Fairness Score; fairness assessment tools and frameworks. Robustness - dimensions of robustness: safety, reliability, resilience, causality; techniques for	Inspired from Certificate Program on Responsible AI-Tour by IIT Madras and Course in Responsible Artificial Intelligence(Course Code-DS5604) by IIT Palakkad. Covered by [3], [4] & [5].	12

	adversarial testing, robustness metrics, robustness assessment tools and frameworks.		
Unit-4 Governing AI	Importance of AI incident reporting; role of standardisation organisations; comparison and critical analysis of current global AI policy and standards initiatives; overview and critical discussion of different codes of practices and principles for AI ethics and their implementation; critical discussion of methods for ethical impact assessment, Critical discussion of methods for ethical design, Interdisciplinary approaches to AI (relevant theories and methods from philosophical ethics, social sciences, and design studies); case study of the EU AI Act.	Inspired from MSt in AI Ethics and Society by University of Cambridge and Certification Program on Responsible & Safe AI systems by IIIT Hyderabad and IIT Madras . Covered by [6] & [8].	12
Reference Books (SHOULD Know)	1. Virginia Dignum, "Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way" Springer Nature, 04-Nov-2019;ISBN-10 : 3030303705, ISBN-13 : 978-3030303709 2. Voeneky S, Kellmeyer P, Mueller O, Burgard W, eds. In: The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspectives. Cambridge Law Handbooks. Cambridge University Press; 2022:iii-iii. 3. Fairness Assessment and Rating of Artificial Intelligence Systems.(2023). https://tec.gov.in/pdf/SDs/TEC%20Standard%20for%20fairness%20assessment%20and%20rating%20of%20AI%20systems%20Final%20v5%202023_07_04.pdf 4. Agarwal, A., Agarwal, H. & Agarwal, N. Fairness Score and process standardization: framework for fairness certification in artificial intelligence systems. AI Ethics 3, 267–279 (2023) https://link.springer.com/article/10.1007/s43681-022-00147-7 5. Agarwal, A., Agarwal, H. A seven-layer model with checklists for standardising fairness assessment throughout the AI lifecycle. AI Ethics (2023) https://link.springer.com/article/10.1007/s43681-023-00266-9 6. EU Artificial Intelligence Act.(2024) https://artificialintelligenceact.eu/the-act/ 7. OECD.(2019) https://oecd.ai/en/ai-principles 8. Jobin, A., Ienca, M. & Vayena, E. The global landscape of AI ethics guidelines. Nat Mach Intell 1, 389–399 (2019). https://doi.org/10.1038/s42256-019-0088-2 9. McGregor, S. (2021, May). Preventing repeated real world AI failures by cataloging incidents: The AI incident database. In Proceedings of the AAAI Conference on Artificial Intelligence (Vol. 35, No. 17, pp. 15458-15463).		
Laboratory Assignments/ Demonstrations			
1	**Structured & Unstructured Data base** generation and norms. Implementations. Platforms. Installations. Querying.		

2	**Bias Detection in Sentiment Analysis**: Analyse sentiment datasets for biases against specific groups
3	**Fair Classification**: Implement and compare fairness-aware classifiers using different fairness constraints
4	**Bias in Facial Recognition**: Evaluate facial recognition systems for demographic biases.
5	**Fairness Metrics Implementation**: Calculate and compare different fairness metrics on a sample dataset
6	**Impact of Pre-processing Techniques**: Apply re-sampling techniques to mitigate bias and evaluate their effectiveness
7	**Adversarial Debiasing**: Implement an adversarial model to reduce bias in predictions.
8	**Fair Representation Learning**: Train models with fairness constraints and analyse learned representations
9	**Bias in Recommendation Systems**: Assess and mitigate bias in recommendation algorithms.
10	**Policy Impact Analysis**: Simulate the impact of different fairness policies on AI system outcomes
11	**Ethical Decision-Making in AI**: Design a decision-making system with ethical constraints and evaluate its fairness.

Subject code	**CE-602**
Subject title	**Intelligent Algorithms**
Credit	**04**
Type of Course	-Core (MTech in CSE) -Professional Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	1. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 2. One Final Evaluation at the End of the Term **50 Marks** 3. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	C programming and debugging concepts, basic concepts of operating systems
Course Objectives	1. To focus on the design of algorithms in various domains 2. To provide a foundation for designing efficient algorithms. 3. To provide familiarity with main thrusts of work in algorithms- sufficient to give some context for formulating and seeking known solutions to an algorithmic problem

Course Outcomes	Bloom's Taxonomy: Level-1 Remember; Level-2 Understand; Level-3 Apply; Level-4 Analyze Level-5 Evaluate; Level-6 Create		
	CO Title	**Level**	**Descriptor**
	CO1: Familiarize students with different algorithmic techniques	L1, L2	Remember, Learn, Understand
	CO2: Apply advanced methods of designing and analyzing algorithms.	L2	Understanding
	CO3: Choose appropriate algorithms and use it for a specific problem	L3	Applying
	CO4: Understand different classes of problems concerning their computation difficulties	L4	Analyzing
	CO5: Implement algorithm, compare their performance characteristics, and estimate their potential effectiveness in applications	L5	

Syllabus Description

Unit	**Details**	**Duration**
Unit-1	**Module:1 Algorithm Design Techniques** Revisit of Greedy algorithms, divide-conquer, dynamic programming. Backtracking: General method, N-queen problem, Subset sum, Graph coloring, Hamiltonian cycles. Branch and Bound: General method, applications -Traveling sales person problem, 0/1 knapsack problem- LC Branch and Bound solution, FIFO Branch and Bound solution. Dynamic Programming **Module:2 Network Flow** Flow Networks, Networks with multiple sources and sinks, Floyd-War shall algorithm, Max Flow and Min Cut, Ford-Fulkerson Method and Edmonds-Karp Algorithm, Bipartite Matching.	9hr
Unit-2	**Module:3 Computational Complexity** Class complexity classes: P, NP, Reductions, NP-completeness and NP-hard, NP-Complete Problems, CNF-SAT and 3SAT, Vertex-Cover and Clique **Module:4 Randomized Algorithms** Las Vegas algorithms, Randomized Quick Sort, Monte Carlo algorithm, Primality Testing **Module:5 Approximation Algorithms** Limits to Approximability, Bin Packing (First fit, Best fit),2 – Approximation algorithm for Metric TSP, Euclidean TSP, Max-SAT and Vertex Cover	12hr
Unit-3	**Module:6 Computational Geometry** Segment-intersection algorithm, Algorithms for finding convex hull: Graham's scan, Gift wrapping Algorithm. Finding the closest pair of points.	10hr

	Module:7 Algorithms for AI Uninformed search, Heuristic search (8 queen and tiling problems), A* and AO* algorithms, Meta-Heuristics **Module 8 Generic Algorithms and Evolutionary Computation** Introduction, Operators, Applications, GA, Fuzzy Logic	
Unit-4	**Module 9: Machine Learning Algorithms** Supervised/Unsupervised, XGBoost, LGBM, Regression, Classification, Neural Networks **Module 10: Cryptographic Algorithms** AES, DES, Hashing, Crypto-Currency Mining Algorithm, Block Chains, RSA, DHA Algorithms **Module 11: High Performance** Multithreading, Parallel Processing, GPU, Linux Clusters, TPU	23hr
Text Books (MUST Know)	1. Han Huang, Zhifeng Hao. "Intelligent Algorithms", 1st Edition, Elsevier, 2024. 2. Russel and Norvig, "Artificial Intelligence : A Modern Approach", 4th Ed, Pearson, 2022. 3. R. Hurbans, "Artificial Intelligence Algorithms", Manning Publishers, 1st Ed, 2020.	
Reference Books (SHOULD Know)	1. M.T.Goodrich and R.Tomassia, 'Algorithm Design: Foundations, Analysis and Internet examples' , John Wiley and sons, 2011. 2. T.H.Cormen, C.E.Leiserson, R.L.Rivest, and C.Stein, 'Introduction to algorithms',4th Edition, MIT Press, 2009. 3. A.Levitin, 'Introduction to the Design and Analysis of Algorithms', Third Edition, Pearson Education, 2012.	

Laboratory Assignments/ Demonstrations

Lab 1	Crypto-Currency Mining
Lab 2	Insertion Sort and Merge Sort: Python Code
Lab 3	Merge Sort and Multi-Threading: Python Code
Lab 4	Random numbers and Linked List: Python Code
Lab 5	Dynamic Programming: Python Code
Lab 6	Decision Tree : Python Code
Lab 7	Graph Algorithms : Python Code
Lab 8	Stable Matching Algorithm: Python Code
Lab 9	Clustering Lloyd's Algorithm: Python Code
Lab 10	Genetic Algorithm: Python Code
Lab 11	Fuzzy Logic: Python Code

Subject Code	CE-603
Subject title	**Deep Neural Networks**
Credit	**04**
Type of Course	-Core (MTech in CSE) -Professional Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	4. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 5. One Final Evaluation at the End of the Term **50 Marks** 6. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	Knowledge of Statistical Techniques, Probability Theory, Data Structures and Algorithms, Programming Language such as Python, Matlab.
Course Objectives	To understand concepts of Neural Network and Deep Learning. To understand how to train Deep Models and Convolutional Networks. To understanding and analyze the related study and refer different latest research views in Latest trend and techniques.
Course Outcomes	Bloom's Taxonomy: Level-1 Remember; Level-2 Understand; Level-3 Apply; Level-4 Analyze Level-5 Evaluate; Level-6 Create

	CO Title	**Level**	**Descriptor**
	CO1 Remembering the basics of Neural Networks and Deep learning	L1, L2	Remember, Learn, Understand
	CO2 Understanding the Different Neural Network Architectures and Deep Learning Methodologies	L2	Understanding
	CO3 Applying different convolution operations, pooling, Functions, and sequence modeling	L3	Applying
	CO4 Analyze Various other Deep Learning architectures like RNN, Autoencoders and GANSs	L4	Analyzing

Syllabus Description

Unit	**Details**	**Books & References**	**Duration**	**COs**
Unit-1	Introduction : Overview of machine learning, linear classifiers, loss functions Optimization : Stochastic gradient descent and contemporary variants, backpropagation	T1, R1	5hr	CO1& CO2

Unit-2	Feedforward networks and training : Activation functions, initialization, regularization, batch normalization, model selection, ensembles.	T1,R1	9hr	CO2
Unit-3	Convolutional neural networks: Fundamentals, architectures, pooling, Visualization, Image Classification, and Object Detection using CNN	T1, R4	16hr	CO3
Unit-4	Recurrent neural networks: Recurrent neural networks (RNN), long-short term memory (LSTM), language models, machine translation, image captioning, video processing, visual question answering, video processing, learning from descriptions, attention	T2, R4	10hr	CO4
Unit-5	Deep generative models: Auto-encoders, generative adversarial networks	T1, R4	5hr	CO4
Text Books (MUST Know)	Ian Goodfellow, Y. Bengio, A. Courville, Deep Learning, MIT Press, 2016. http://www. deeplearningbook.org. Michael Nielsen, Neural Networks and Deep Learning, Determination Press, 2015. http://neuralnetworksanddeeplearning.com/			
Reference Books (SHOULD Know)	K. P. Murphy, Machine Learning: A Probabilistic Perspective, MIT Press, 2012. C. M. Bishop, Pattern Recognition and Machine Learning, Springer, 2006. A National Initiative on AI Skilling and Research (leadingindia.ai) NPTEL Course Lecture Material: Deep Learning Part-1 By Dr. Mitesh Kapra, IIT Chennai.			

Laboratory Assignments/ Demonstrations

Lab 1	Implementation of Linear Classifier using ML	Unit 1	02 hours	CO1 & 2
Lab 2	Implementation of Activation Functions and analyze the significance of Weight and Bias for ML Model	Unit 2	02 hours	CO1 & 2
Lab 3	Implementation of Perceptron Model for Binary Logic.	Unit 2	02 hours	CO1 & 2
Lab 4	Implementation of XOR using Multi-Layer Perceptron	Unit 2	02 hours	CO1 & 2
Lab 5	Implementation of Convolutional Neural Networks	Unit 3	02 hours	CO3
Lab 6	Object Detection using CNNs	Unit 3	02 hours	CO3
Lab 7	Image Classification Using CNNs	Unit 3	2	CO3
Lab 8	Analyzing various CNN Architectures	Unit 3	2	CO3
Lab 9	Implementing RNNs and LSTM	Unit 4	2	CO4

Lab 10	Analyzing CNNs and RNNs for Deep Learning Applications	Unit 5	2	CO4

Subject Code	**CE-604**		
Subject title	**Practical Machine Learning**		
Credit	**04**		
	-Core (MTech in CSE) -Professional Open Elective for All Engineering and Science disciplines		
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.		
Evaluation Pattern	1. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 2. One Final Evaluation at the End of the Term **50 Marks** 3. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**		
Total Marks	100 Marks		
Prerequisite	Knowledge of Statistical techniques, Linear algebra and computer programming knowledge is required.		
Dept	CSE		
Course Objectives	To provide the knowledge of Python programming language as it applies to data analytics. Skills will be developed for Data Analysis with Python and develop products in Python. Student will learn various ML techniques including Supervised, unsupervised classification and regression analysis, Artificial Neural Networks, etc. Student will learn Python Programming for implementing these algorithms on standard datasets		
Course Outcomes	Bloom's Taxonomy: Level-1 Remember; Level-2 Understand; Level-3 Apply; Level-4 Analyze Level-5 Evaluate; Level-6 Create		
	CO Title	**Level**	**Descriptor**
	CO 1 - Students will be able to understand ML paradigms and various Supervised, unsupervised classification and regression analysis methods. (PO1,PO2, PO3, PSO2)	L1, L2	Remember, Learn, Understand
	CO2: Students will be able to understand various ML algorithms like and analyse their applications in real world (PO1,PO2, PO3, PSO2)	L2	Remember, Learn, Understand
	CO3: Students will be able to understand advanced ML algorithms and techniques etc. (PO1,PO2, PO3, PSO2)	L3	Remembering, Understanding, Analysing
	CO4: Students will be capable of applying their ML knowledge and skills to solve engineering problems in various domains using ML programming languages(PO1, PO2, PO3, PSO1, PSO2)	L4	Applying, Analysing

Syllabus Description				
Unit	**Details**	**Books & References**	**Duration**	**COs**
Unit-1	Data Analytics Foundations: R programming, Python Basics -Expressions and Variables, String Operations, Lists and Tuples, Sets, Dictionaries Conditions and Branching, Loops, Functions, Objects and Classes, Reading/Writing files, Hand ling data with Pandas, Scikit Library, Numpy Library, Matplotlib, scikit programming for data analysis, setting up lab environment, study of standard datasets. Introduction to Machine Learning- Applications of Machine Learning, Supervised, unsupervised classification and regression analysis	Textbooks -1,2	12 Hrs	CO1
Unit-2	Python libraries suitable for Machine Learning Feature Extraction. Data pre-processing, feature analysis etc., Dimensionality Reduction & Feature Selection Methods, Linear Discriminant Analysis and Principal Component Analysis, tackle data class imbalance problem	Textbooks -2,3	12 Hrs	CO2
Unit-3	Supervised and regression analysis, Regression, Linear Regression, Non-linear Regression, Model evaluation methods, Classification, K-Nearest Neighbor, Naïve Bayes, Decision Trees, Logistic Regression, Support Vector Machines, Artificial Neural Networks, Model Evaluation. Ensemble Learning, Convolutional Neural Networks, Spectral Embedding, Manifold detection and Anomaly Detection	Textbooks -2,3,4	12 Hrs	CO2
Unit-4	Unsupervised classification K-Means Clustering, Hierarchical Clustering, Density-Based Clustering, Recommender Systems- Content-based recommender systems, Collaborative Filtering, machine learning techniques for standard dataset, ML applications, Case Study: Image spam detection	Textbooks -4-5, / References -1-4	12 Hrs	CO3
	LAB/ Assignments/Student Presentations [2T/P per week]			
Text Books (MUST Know)	1. Building Machine Learning Systems with Python - Willi Richert, Luis Pedro Coelho 2. Learning scikit-learn: Machine Learning in Python - Raúl Garreta, Guillermo Moncecchi 3. Machine Learning: An Algorithmic Perspective - Stephen Marsland 4. Sunita Vikrant Dhavale, “Advanced Image-based Spam Detection and Filtering Techniques”, IGI Global, 2017 5. Trevor Hastie, Robert Tibshirani, Jerome Friedman - The Elements of Statistical Learning: Data Mining, Inference, and Prediction. Second Edition. February 2009			

Reference Books (SHOULD Know)	1. Stuart Russell, Peter Norvig (2009), "Artificial Intelligence – A Modern Approach", Pearson Elaine Rich & Kevin Knight (1999), "Artificial Intelligence", TMH, 2nd Edition 2. NP Padhy (2010), "Artificial Intelligence & Intelligent System", Oxford 3. ZM Zurada (1992), "Introduction to Artificial Neural Systems", West Publishing Company 4. Research paper for study (if any) - White papers on multimedia from IEEE/ACM/Elsevier/Spinger/ NVidia sources.

Laboratory Assignments/ Demonstrations

1	Study and implement algorithms for data pre-processing and data cleaning	Unit -1	02 hours	CO1, CO3, & CO4
2	Study and implement algorithms for data feature selection reduction.	Unit -1	02 hours	CO1, CO3, & CO4
3	Study and Implement Linear Regression Algorithm for any standard dataset	Unit -2	02 hours	CO2, CO3, & CO4
4	Study and Implement unsupervised clustering Algorithms for any standard dataset	Unit -3	02 hours	CO1, CO3, & CO4
5	Study and Implement KNN for any standard dataset	Unit -3	04 hours	CO1, & CO4
6	Study and Implement ANN for any standard dataset	Unit -3	02 hours	CO2, & CO3
7	Study and Implement PCA for any standard dataset	Unit -3	02 hours	CO3, & CO4
8	Case Study: Use of ML along with Fuzzy Logic/ GA/PSO/ACO to solve real world Problem	Unit -4	04 hours	CO2, & CO3
9	Mini assignment: Apply ML to solve any real world problem	Unit -4	04 hours	CO2, & CO4
10	ML Practice Test – 1 Quiz	Unit -1,2,3,4	02 hours	CO1,CO2, CO3, & CO4

Subject code	**CE-605**
Subject title	**Mathematics for Machine Learning**
Credit	**04**
Type of Course	-Core (MTech in CSE)
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	03 – monthly test + 01 Final Evaluation

Total Marks	100
Prerequisite	Machine Learning; Linear Algebra; Probability & Statistics, NLP
Dept	SoCE&MS
Course Objectives	Machine Learning refers to the automated identification of patterns in data. As such it has been a fertile ground for new statistical and algorithmic developments. The purpose of this course is to provide a mathematically rigorous introduction to these developments with emphasis on methods and their analysis
Course Outcomes	Bloom's Taxonomy: Level-1 Remember; Level-2 Understand; Level-3 Apply; Level-4 Analyze Level-5 Evaluate; Level-6 Create

	CO Title	**Level**	**Descriptor**
	CO1 Remembering the basics of Mathematical Machine Learning	Level 1 & 2	Remembering, Understanding
	CO2 Understanding various domains of Mathematical Machine Learning	Level 2	Understanding
	CO3 Applying different concepts of Linear Algebra, Probability, Optimization and Dimensionality Reduction for Practical Problems	Level 3	Applying
	CO4 Analyze Mathematical Machine Learning based Models and fine tune them for real datasets.	Level 4	Analyzing

Syllabus Description

Unit	**Details**	**Books & References**	**Duration**	**COs**
Unit-1	**Linear Algebra and Matrix Decomposition:** Scalars, Vectors, Matrices and Tensors, Multiplying Matrices and Vectors, Identity and Inverse Matrices – Linear Dependence and Span – Norms – Special kinds of matrices and vectors – Determinant and Trace, Eigenvalues and Eigenvectors, Cholesky Decomposition, Eigen decomposition and Diagonalization , Singular Value Decomposition, Matrix Approximation, Differentiation of Univariate Functions, Partial Differentiation and Gradients, Gradients of Vector-Valued Functions, Gradients of Matrices, Useful Identities for Computing Gradients	T1	12 Hr	CO1& CO2
Unit-2	**Probabilistic Machine Learning:** Fundamentals of Probability, Univariate and Multivariate Models, Joint Distributions,	T2	12Hr	

	Basian Statistics and Regularization Methods, Decision and Information Theory.			
Unit-3	**Optimizations:** Introduction to Optimization methods, first and second order optimization, Stochastic gradient descent, Constrained Optimization, Black box and derivative free optimization.	T2	12 Hr	CO3
Unit-4	**Dimensionality Reduction with Principal Component Analysis:** Problem Setting, Maximum Variance Perspective, Projection Perspective, Eigenvector Computation and Low-Rank Approximations, PCA in High Dimensions, Key Steps of PCA in Practice, Latent Variable Perspective	T1,	12 hr	CO4
Text Books (MUST Know)	**T1: "Mathematics for Machine Learning",** By Marc Peter Deisenroth, A. Aldo Faisal, Cheng Soon, Cambridge University Press, 2020 **T2: "Probabilistic Machine Learning: An Introduction",** By Kevin P. Murphy, The MIT Press Cambridge, Massachusetts London, England, 2022			
Reference Books (SHOULD Know)	https://mltechniques.com/2022/06/13/math-for-machine-learning-12-must-read-books/ Model-Based Machine Learning, By John Winn, CRC Press, 2023.			

Course Code	**AM 607**
Course Title	**Mathematics for Engineers**
Credit	**04**
TeachingScheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	03 monthly tests + 01 final evaluation + assignments for internal assessment
Total Marks	100
Prerequisite	NIL
Course Instructor	Faculty from Math Dept
Course offered from Mathematics Department, DIAT	
Syllabus: **Elements of Probability and Statistics:** Basic concepts of Probability, Discrete Probability Distributions (Binomial, Poisson etc.),Continuous Probability Distributions (Normal, Exponential, etc.,). **Components of Operations Research:** Introduction to Operations Research, Linear programming (Simplex Method, Revised Simplex Method, Dual simplex, Duality theory),Transportation Models.	

Linear Algebra:

General (real) vector spaces, Subspaces, Linear Independence of Vectors, Basis and Dimension, Linear Transformations, Span, Norms,Orthogonal basis and Gram-Schmidt Orthogonalization.

Ordinary Differential Equations :

Review of solution methods for first order as well as second order equations, Power Series methods. Higher Order Linear Equations,Boundary Value Problems for Second Order Equations.

Transform Techniques :

Overview of Laplace transforms, Fourier Transforms, Z transform.

Numerical Methods for ODE and P.D.E.:

Taylor series method – Euler and Modified Euler methods – Runge-Kutta method. Parabolic, Hyperbolic and Elliptic Equations using finite difference method

Text/References:

1. Advanced Engineering Mathematics, 11th Ed, 2010, Erwin Kreyszig, Wiley Eastern.
2. Linear Algebra and its Applications, 4th Ed., 2008, Gilbert Strang, Academic Press.
3. Numerical Methods for Scientists and Engineers, Joe D. Hoffman, Marcel Dekker Inc.
4. Numerical Methods for Engineers, Sixth Edition, Steven Chapra and Raymond Canale, McGraw-Hill Education
5. Elements of Numerical Analysis, 2nd Edition, Radhey S. Gupta**,** Cambridge University Press
6. Numerical Solutions of Partial Differential Equations: An Introduction, 2nd Ed., 2005, K. W. Morton, D. F. Mayers, CambridgeUniversity Press.
7. Operations Research: An Introduction, 9th Ed., 2010, Taha, H.A., Prentice Hall of India.
8. Optimization Theory and Applications, 2nd Ed., 1984, S.S. Rao, Wieley Eastern Ltd.
9. Introduction to probability and statistics for engineers and scientists, 4th Ed., 2009, Ross S M, Acdemic Press.
10. An Introduction to Probability Theory and its Application, 3rd Ed., 2012, William Feller, John Wiley India Pvt. Ltd.
11. Differential Equations and Dynamical Systems, Texts in Applied Mathematics, L. Perko, 3rd Ed., Vol. 7, 2006, Springer Verlag,New York.
12. S. Gupta.. Calculus of Variation, Prentice Hall of India Pvt. Ltd.

Course Code	**PGC-601**
Course Title	**IPR and Research Methodology**
Credit	**02**
Teaching Scheme	Lectures: 02 hours/week
Evaluation Pattern	03 monthly tests + 01 final evaluation + assignments for internal assessment
Course Instructor	**Institute-level conduct**

Syllabus Contents:

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

Unit 2: Effective literature studies approaches, analysis

	Plagiarism, Research ethics, **Unit 3:** Effective technical writing, how to write report, Paper Developing a Research Proposal, Format of research proposal, a presentation and assessment by a review committee **Unit 4:** Nature of Intellectual Property: Patents, Designs, Trade and Copyright. Process of Patenting and Development: technological research, innovation, patenting, development. International Scenario: International cooperation on Intellectual Property. Procedure for grants of patents, Patenting under PCT. **Unit 5:** Patent Rights: Scope of Patent Rights. Licensing and transfer of technology. Patent information and databases. Geographical Indications. **Unit 6:** New Developments in IPR: Administration of Patent System. New developments in IPR; IPR of Biological Systems, Computer Software etc. Traditional knowledge Case Studies, IPR and IITs.
References:	1. Stuart Melville and Wayne Goddard, "Research methodology: an introduction for 2. science & engineering students'" 3. Wayne Goddard and Stuart Melville, "Research Methodology: An Introduction" 4. Ranjit Kumar, 2nd Edition, "Research Methodology: A Step by Step Guide for 5. Halbert, "Resisting Intellectual Property", Taylor & Francis Ltd,2007. 6. Mayall, "Industrial Design", McGraw Hill, 1992. 7. Niebel, "Product Design", McGraw Hill, 1974. 8. Asimov, "Introduction to Design", Prentice Hall, 1962. 9. Robert P. Merges, Peter S. Menell, Mark A. Lemley, " Intellectual Property in New Technological Age", 2016. 10. T. Ramappa, "Intellectual Property Rights Under WTO", S. Chand, 2008

Subject Code	**CE-611**
Subject title	**Computer Vision**
Credit	**04**
Type of Subject	-Core (MTech in CSE) -Professional Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	• Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** • One Final Evaluation at the End of the Term **50 Marks** • Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	Statistical techniques, Linear algebra and computer programming knowledge is required.
Dept	CSE

Course Objectives	To introduce students the fundamentals of image formation; To introduce students the major ideas, methods, and techniques of computer vision and pattern recognition; To develop an appreciation for various issues in the design of computer vision and object recognition systems; and To provide the student with programming experience from implementing computer vision and object recognition applications.		
Course Outcomes	Bloom's Taxonomy: Level-1 Remember; Level-2 Understand; Level-3 Apply; Level-4 Analyze Level-5 Evaluate; Level-6 Create		
	CO Title	**Level**	**Descriptor**
	CO1: Students will be able to understand and apply image processing techniques including filtering operations, thresholding techniques, edge detection techniques etc. (PO1, PO2, PO3, PSO2)	L1, L2	Remember, Understand
	CO2: Students will be able to understand and extract image features using techniques like corner and interest point detection, shape analysis, fourier descriptors, Ransac, GHT etc. (PO1, PO2, PO3, PSO2)	L3	Remember, Understand Analyse
	CO3: Students will be able to understand and learn how the extracted features can be used to solve problems in various computer vision related applications. (PO1, PO2, PO3, PSO2)	L3	Remember, Understand Analyse
	CO4: Students will be capable of applying their knowledge and skills to solve engineering problems in computer vision related domain. (PO1, PO2, PO3, PSO2)	L4	Apply, Analyse

Syllabus Description

Unit	**Details**	**Books & References**	**Duration**	**COs**
Unit-1	Image processing foundations: Review of image processing techniques, classical filtering operations, thresholding techniques, edge detection techniques, mathematical morphology, texture analysis, Shapes and regions: Binary shape analysis – connectedness – object labeling and counting – size filtering – distance functions – skeletons and thinning	Textbooks -1	12L	CO1
Unit-2	Corner and interest point detection, deformable shape analysis – boundary tracking, procedures – active contours – shape models and shape recognition – centroidal profiles – handling occlusion – boundary length measures – boundary descriptors – chain codes, Fourier descriptors – region descriptors – moments, Hough transform: Line detection – Hough Transform (HT) for line detection – foot-of-normal method – line localization – line fitting	Textbooks -2	12L	CO2

Unit-3	Case study: spatial matched filtering – GHT for ellipse detection – object location – GHT for feature collation RANSAC for straight line detection – HT based circular object detection – accurate center location – speed problem – ellipse detection	Textbooks -2,3	12L	CO2
Unit-4	Case Study: Image based spam detection, Case Study: CV Applications - Face detection – Face recognition – Eigen faces, Case Study: CV Applications - human gait analysis, Case Study: CV based Surveillance Applications, Concepts of stereo vision	Textbooks/ References -4-8	12L	CO3
	LAB/ Assignments/Student Presentations [2T/P per week]		02L/Week	CO4
Text Books	1. E. R. Davies, "Computer & Machine Vision", Fourth Edition, Academic Press, 2012. 2. R. Szeliski, "Computer Vision: Algorithms and Applications", Springer 2011. 3. Simon J. D. Prince, "Computer Vision: Models, Learning, and Inference", Cambridge University Press, 2012. Mark Nixon and Alberto S. Aquado, "Feature Extraction & Image Processing for Computer Vision", Third Edition, Academic Press, 2012.			
Reference Books	1. D. L. Baggio et al., "Mastering OpenCV with Practical Computer Vision Projects", Packt Publishing, 2012. 2. Jan Erik Solem, "Programming Computer Vision with Python: Tools and algorithms for analyzing images", O'Reilly Media, 2012. 3. Sunita Vikrant Dhavale, "Advanced Image-based Spam Detection and Filtering Techniques", IGI Global, 2017 4. Research paper for study (if any) - White papers on multimedia from IEEE/ACM/Elsevier/Spinger/ NVidia sources.			

Laboratory Assignments/ Demonstration

1	Introduction to Digital Image Processing using python	Unit -1	02 hours	CO1, CO2,CO3, & CO4
2	Study and Implement Image Transformation Techniques	Unit -1	02 hours	CO1, CO3, & CO4
3	Study and Implement Image Transformation Techniques	Unit -1	02 hours	CO2, CO3, & CO4
4	Study and Implement Edge Detection Techniques	Unit -1	02 hours	CO1, CO3, & CO4
5	Study and Implement Image Thresholding Transform	Unit -1	04 hours	CO1, & CO4
6	Study and Implement Morphological Operations	Unit -2	02 hours	CO2, & CO3
7	Study and Implement Harris Corner Point Detection	Unit -2	02 hours	CO3, & CO4
8	Study and Implement SIFT	Unit -3	04 hours	CO2, & CO3

9	Mini assignment: Apply CV techniques to solve any real world problem/ Presentations	Unit -4	04 hours	CO2, & CO4
10	CV Practice Test -1Quiz/ Presentations	Unit -4	02 hours	CO1,CO2, CO3, & CO4

Subject Code	**CE-612**
Subject title	**Adversarial and Generative AI**
Credit	**04**
Type of Course	-Core (MTech in CSE) -Professional Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	03 – monthly test + 01 Final Evaluation
Total Marks	100
Prerequisite	Machine Learning; Multivariable Calculus; Linear Algebra; Probability & Statistics.
Dept	SoCE&MS
Course Objectives	To understand the concepts and needs of Generative modelling and Learn the concepts of probability and modelling. To implement the learned concepts to generate the data related to specific applications of image and Video .
Course Outcomes	Bloom's Taxonomy: Level-1 Remember; Level-2 Understand; Level-3 Apply; Level-4 Analyze Level-5 Evaluate; Level-6 Create

CO Title	**Level**	**Descriptor**
CO1 Remembering the basics of Generative Modelling	Level 1 & 2	Remembering, Understanding
CO2 Understanding the different types of Generative Models	Level 2	Understanding
CO3 Applying different GAN architectures for Image and Video Data	Level 3	Applying
CO4 Analyze Various GAN architectures for different applications	Level 4	Analyzing

Syllabus Description

Unit	**Details**	**Books & References**	**Duration**	**COs**

Unit-1	Introduction to Generative AI : What is generative AI?, Types of generative models, Applications of generative AI,Probabilistic Models: Introduction to probability theory, Bayesian networks, Markov random fields.	T1, R1	10 Hr	CO1& CO2
Unit-2	Autoencoders: Basics of autoencoders, Variational autoencoders (VAEs), Autoencoder-based	T1, R1	8 Hr	
Unit-3	Deep Generative Models: Introduction to deep generative models, Deep Boltzmann Machines (DBMs), DeepBelief Networks (DBNs), Adversarial attacks on generative models, Neural Ordinary Differential Equations (ODEs)	T1, R4	14 Hr	CO3
Unit-4	Applications of GANs for Image Generation, Super-resolution and Video Prediction.	T1, R4	10hr	CO4
Text Books (MUST Know)	Ian Goodfellow, Y. Bengio, A. Courville, Deep Learning, MIT Press, 2016. http://www. deeplearningbook.org.			
Reference Books (SHOULD Know)	Probabilistic Graphical Models, 2009, D. Koller, and N. Friedman, MIT Press. A National Initiative on AI Skilling and Research (leadingindia.ai) NPTEL Course Lecture Material: Deep Learning Part-II By Dr. Mitesh Kapra, IIT Chennai.			

Laboratory Assignments/ Demonstrations

Lab No	Lab Experiment	Unit	Hours	CO's
1	Implementation of Discriminator using various CNN Models	I	4	CO3
2	Implementation of Generators using Variational Auto Encoders and Attention Models	II	4	CO3
3	Implementation of GANs using Up-sampling and Down-Sampling	III	4	CO4
4	Case Studies on Radar Image Generation, Astronomical Image Generation, Activity Prediction	IV	4	CO4

SEMESTER II ELECTIVE COURSES

Subject code	CE-613
Subject title	**Large Language Models**
Credit	**04**
Type of Course	-Core (MTech in CSE)
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	03 – monthly test + 01 Final Evaluation
Total Marks	100
Prerequisite	Machine Learning; Linear Algebra; Probability & Statistics, NLP
Dept	SoCE&MS
Course Objectives	This course is intended to prepare the students for performing cutting-edge research in natural language processing, especially topics related to pre-trained language models by understanding the state-of-the-art models, their capabilities, and limitations.
Course Outcomes	Bloom's Taxonomy: Level-1 Remember; Level-2 Understand; Level-3 Apply; Level-4 Analyze Level-5 Evaluate; Level-6 Create

	CO Title	**Level**	**Descriptor**
	CO1 Remembering the Probabilistic theory of LLMs	Level 1 & 2	Remembering, Understanding
	CO2 Understanding Modeling Foundations and Neural Network Models for LLMs	Level 2	Understanding
	CO3 Applying Transfer Learning for Training, Fine Tuning and Inference of LLMs	Level 3	Applying
	CO4 Analyze LLMs for Security & AI Safety	Level 4	Analyzing

Syllabus Description

Unit	**Details**	**Books & References**	**Duration**	**COs**
Unit-1	Introduction, Language Processing with Python, Accessing Text Corpora, Conditional Frequency Distribution, Lexical Resources. Categorizing and Tagging Words, Tagger, Tagged Corpora, Automatic Tagging, NGram Tagging, Transformation based Tagging	T3	10hr	**CO1**

	Learning to classify Text, Supervised Classification, Evaluation, Decision Trees, Naïve Bayes Classifier, Maximum Entropy Classifiers, Extracting Information from Text, Information Extraction, Chunking, Evaluation of Chunking, Recursion, Relation			
Unit-2	Introduction and Overview; **Probabilistic Foundations:** Basic Measure Theory, Defining a Language Model, Tight Language Models, The Language Modeling Task **Modeling Foundations:** Finite-State Language Models, Recurrent Neural Language Models	T1	8hr	**CO2**
Unit-3	**Neural Network Modeling:** Representational Capacity of RNN LMs, Transformer-based Language Models, Transformer-based Language Models, Representational Capacity of Transformer-based Language Models, Tokenization, Generating Text from a Language Model	T1	10hr	CO2
Unit-4	**Training, Fine Tuning and Inference**: Transfer Learning, Parameter efficient finetuning, In-context learning, Prompting, zero-shot, instruction tuning Applications and the Benefits of Scale: Multimodality, Retrieval augmented Language Models	T2	10hr	CO3
Unit-5	**Security:** Instruction tuning and RLHF Harms & Ethics, Security & Adversarial examples, Prompt injections, Data poisoning, backdoors and model stealing, Privacy in ML, Memorization + Differential Privacy, Data lifecycle, Explainability, Interpretability, AI Safety	T2	10hr	CO4
Text Books (MUST Know)	Large Language Models, Spring 2023 | Rycolab T1: LLM Course Notes Part 1 T2: LLM Course Notes Part 2 T3: S.Bird, E Klein and E Loper, —Natural Language Processing with Python‖, O'Reilly, 2009.			
Reference Books (SHOULD Know)	R1: Deep Learning (deeplearningbook.org) R2: Introduction to Natural Language Processing (Eisenstein) R3: COS 597G: Understanding Large Language Models (princeton.edu)			

Subject Code	CE695A
Subject Title	**Cyber Physical Systems**
Credit	**04**
Type of Sub	Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	7. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 8. One Final Evaluation at the End of the Term **50 Marks** 9. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	None. First 10 hours will be devoted for Prerequisite learnings related to basics of Databases (04 hours), Computer Networks (02 Hours), Operating System (02 Hours), Trends in evolutions of Compute-Devices (02 Hours)
Dept	CSE
About the Course	This course examines a new class of computational systems called Cyber-Physical Systems CPS. Such systems have the potential to provide far-reaching benefits in addressing some of the toughest problems we face as a society, such as: reducing healthcare costs, minimizing traffic congestion, and constructing zero-net energy buildings. Four important features characterize CPS: their ability monitors the underlying physical environment, reason about the monitored data, control the physical environment through actuation, in a coordinated manner using a communication medium. It can be seen in CPS, the computational element (cyber) and the environment (physical) are tightly coupled, with one influencing the other. CPS sits at the confluence of several traditional disciplines, such as: embedded systems, real-time systems, sensor networks, control and hybrid systems, and security. It presents many challenging problems and opportunities for research. With guidance from the professor, students will survey recent CPS publications, develop an aptitude. Readings will include papers on CPS applications (e.g., Body Area Networks, smart automobiles, and energy-efficient buildings), issues involved in designing CPS (e.g., monitoring, communication, and control), and how to ensure that the designed systems satisfy certain essential properties (e.g., safety and security). CPS combine cyber capabilities (computation and/or communication) with physical capabilities (motion or other physical processes). Cars, aircraft, and robots are prime examples, because they move physically in space in a way that is determined by discrete computerized control algorithms. Designing these algorithms to control CPSs is challenging due to their tight coupling with physical behavior. At the same time, it is vital that these algorithms be correct, since we rely on CPSs for safety-critical tasks like keeping aircraft from colliding, its role in Command & Control environments. To meet end-user, Administrator & System Designer perspectives, develop skill sets to be resourceful in knowledge & information systems. Enhance analytical capabilities to evaluate a domain specific and technical area. Multi-Disciplinary Course useful to any engineering discipline who are keen to contribute in digitization, like be it smart cities, smart telemedicine systems, automated and autonomous systems.
Course Outcomes	Bloom's Taxonomy:

	Level-1 Remember; Level-2 Understand; Level-3 Apply; Level-4 Analyze Level-5 Evaluate; Level-6 Create			
	CO Title	**Level**	**Descriptor**	**Out come**
	CO1: Students will be able to understand the scope of applications of CPS.	L1, L2	Remember, Learn, Understand	20%
	CO2: Students will be able to analyse the various components of CPS	L3, L4	Apply, Analyse	20%
	CO3: Students will apply mechanisms to enable autonomous and self-organising techniques	L4, L5	Analyse, Evaluate	20%
	CO4: Students will be capable of applying their knowledge and skills to solve engineering problems in cyber and information security domain along with scope to apply AIML and build secure digitized systems. (PO1, PO2, PO3, PSO1, PSO2)	L5, L6	Evaluate, Create	40%
Summary of the Course Out Come	At the end of the course, a student will understand the concepts of CPS. Develop skills to relate a CPS as a feedback system along with its designing, modelling and implementation challenges. Evaluate the requirements to address emerging areas of digitization, AIML, and Secure environments.			
Syllabus Description				
Basics & Preliminaries	Role of Basic and Advanced Data Structures in Data Models, Types of Data Models, Basic Dictionary Data Types; Algorithms and basics of analysis, OS & Algorithms in Parallel Environments. Protocols of Computer Networks Preliminaries, Concerns for Data Security and Privacy	Cormen et al,Horowitz Sahani, BipinDesai, Korth et al. Kurose Ross	10 Hours	CO1, PO1
Unit-1	CPS**:** Introduction Main Concepts, Challenges; Background role of Computer Networks, Data, Algorithms	Text Book-1, Ch-1	08 Hours	CO1, CO2, PO1
Unit-2	Self-organising Systems, Self-organisation in Natural Systems Inspiring Self-organising Software,	Text Book-1, Ch-2, 3	04 Hours	CO1, PO1
Unit-3	Agents and Multi-Agent Systems Computing trends, Data device proliferation, Confluence of trends	Text Book-1, Ch-4	06 Hours	CO1 CO2, PO1
Unit-4	Technological and economic drivers Self-organisation Mechanisms, Stigmergy, Gossip, Trust and Reputation for Successful Software Self-organisation, Cooperation , Immune Systems, Holonic Multi-Agent Systems Engineering Artificial Self-organising Systems	Text Book-1, Ch-4, 5	06 Hours	CO3, PO2

Unit-5	Engineering Self-organising Systems, Middleware Infrastructures for Self-organising Pervasive Computing Systems	Text Book-1, Ch 5,6,7,8	06 Hours	CO3, PO2
Unit-6	CPS design Standards, Time Models, CPS Special Interest Groups and Mitre Commendations in Design and developments	Weblink References	06 Hours	C04, PO4
Unit-7	Applications of Self-organising Software, Self-organisation in Constraint Problem Solving, Adaptive Trust Management, Security in Artificial Systems Project Cases: SCADA, Industry 4.0 applications, Telemedicine, Environment Monitoring, IoTs, etc.	Text book-1, Ch-8,9	06 Hours	CO1, CO4, PO1, PO3
Text Books (MUST Know)	Text Books 2. Self-Organising Software from Natural to artificial Adaptation, Di- MarzoSerugendo, ;Gleizer, M-p; Karageorgos, A (Eds), 2011, XVIII,462P; Hardcover ISBN:978-3642-17347-9		Must Know	
Reference Books (SHOULD Know)	Reference Book-1 4. "Principles of Cyber-Physical Systems" - Rajeev Alur, MIT Press, 2015 5. Data Mining, Jiawei Han & Micheline Kamber, 2nd edition, Elsevier, 2006 6. Kurose and Ross, Top Down Approach of Computer Networks, Prentice Hall, 8th Edition 2021.		Should Know	
Consortium, e-books and Web Link references (SHOULD/ Could Know)	5. https://iveybusinessjournal.com/publication/why-big-data-is-the-new-competitive-advantage/https://www.cdsaonline.org/cps-standard/ 6. https://pages.nist.gov/cpspwg/ 7. International Association for Automation 8. Research Papers shared by the subject incharge		Should and May know	
Laboratory Assignments/ Demonstrations				

LAB Assignments	*Each student will work on unique case study. Will require approval of the same at the beginning. Report submission is essential for each Lab Assignment.			
1	Describe the Use Case*. Model the case study. Abstract.	Unit-1	02 hours	CO1
2	Modelling Tools exploration and implementation of the subsystems/ systems of the case study.	Unit-2	02 hours	CO2
3	Depiction of Agents in the designed model, and modelling their state, transitions and parameters status. Any one scenario for automous execution using algorithms.	Unit-3 & 4	02 hours	C03
4	Implement and apply Multi-Agent Systems. Enumerate the challenges, risks and mitigations.	Unit 4 & 5	02 hours	CO3
5	Implement and apply Multi-Agent Systems. Enumerate the challenges, risks and mitigations. Develop the methods to audit and parameters of importance. Generate the incidence response reports.	Unit 4 & 5	02 hours	CO4
6	Implement and apply Multi-Agent Systems. Enumerate the challenges, risks and mitigations. Specify the security concern and mitigation technique. Generate the incidence response reports.	Unit 6	02 hours	CO4
7	Create use case environment, implement & perform intra and Inter-system mappings.	Unit 6	02 hours	CO4
8	Create model and implement any one security feature to demonstrate cyber security concern, intra and inter and mitigation.	Unit-7	02 hours	CO4
9	Study of Research paper on the assigned topic and its presentation.	Unit 1 to 7	Sem	CO4
10	Mini-project. Implementation and Demonstration. Report Submission is essential	Unit 1 to 7	Sem	CO4

Subject Code	**CE630**
Subject title	**Virtual Reality**
Credit	**04**
Type of Subject	-Core (MTech in CSE) -Professional Open Elective for All Engineering and Science disciplines

Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.		
Evaluation Pattern	1. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 2. One Final Evaluation at the End of the Term **50 Marks** 3. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**		
Total Marks	100 Marks		
Prerequisite	Basic Operating systems and Computer Programming, Computer Graphics knowledge is required.		
Dept	CSE		
Course Objectives	Understanding basic issues, concepts, principles and mechanisms in Virtual Reality. • Definition of VR • Applications of VR • VR/AR/MR • Hardware/Software • Human Physiology and Perception • Light and Optics • Human Physiology of Vision • Visual Perception, Visual Rendering • Motion in Real and Virtual Worlds • Tracking and Interaction • Audio, • Evaluating VR Systems • Current trends in VR		
Course Outcomes	Bloom's Taxonomy: Level-1 Remember; Level-2 Understand; Level-3 Apply; Level-4 Analyze Level-5 Evaluate; Level-6 Create		
	CO Title	**Level**	**Descriptor**
	CO1: Students will be able to understand and apply Virtual Reality Concepts along with various applications. (PO1, PO3, PSO1)	L2	Remember, Understand
	CO2: Students will be able to understand and apply Virtual Reality concepts, hardware, software, standards and policies required for various applications. (PO1,PO2, PO3, PSO1)	L3,	Remember, Understand Analyse
	CO3 - Students will be able to understand the importance of implementation of Virtual Reality Systems, Applications with Benefits and limitations(PO1, PO3, PSO1)	L2	Remember, Understand
	CO4: Students will be capable of applying their knowledge and skills to solve engineering problems in Virtual Reality. (PO1, PO2, PO3, PSO1, PSO2)	L4	Apply, Analyse

Syllabus Description				
Basics & Preliminaries	Details	Books & References	Duration	COs
Unit-1	Introduction, Definition, Applications	Lavalle, Chap1	3L	1,2
Unit-2	Bird's Eye View, Hardware, Software, Human Physiology and Perception	Lavalle, Chap2	3L	1,2
Unit-3	Geometry of Virtual Worlds, Geometric models, Viewing Transformations, Chaining Transformations	Lavalle, Chap 3	4L	1,2
Unit-4	Light and Optics, Lenses, optical aberrations, Human Eye, Cameras, displays	Lavalle, Chap 4	4L	1,2
Unit-5	Physiology of Human Vision: Cornea, Photoreceptors, Eye Movements, Implications for VR	Lavalle, Chap 5	3L	1,2
Unit-6	Visual Perception: Perception of Depth, Perception of Motion, Perception of Color, Combining sources of information	Lavalle, Chap 6	4L	1,2,3
Unit-7	Visual Rendering: Ray tracing and Shading models, Rasterization, Correcting optical distortions, Improving latency and frame rates, Immersive photos and videos	Lavalle, Chap 7	4L	1,2
Unit-8	Motion in Real and Virtual Worlds: Velocities and accelerations, Vestibular system, Physics in virtual world, Mismatched motion and vection	Lavalle, Chap 8	4L	1.2
Unit-9	Tracking: Tracking in 2D, Tracking in 3D, Tracking position and orientation, Tracking attached bodies, 3D scanning of environment	Lavalle, Chap 9	4L	1,2
Unit-10	Interaction: Motor programming and remapping, Locomotion and manipulation,	Lavalle, Chap 10	3L	1,2,3

	social interaction and other interaction mechanisms			
Unit-11	Audio: Physics and sound, physiology of human hearing, Auditory perception, Auditory hearing	Lavalle, Chap 11	3L	1,2
Unit-12	Evaluation of VR Systems and Experiences: Perceptual training, recommendation for developers, Comfort and VR Sickness, Experiments on Human Subjects	Lavalle, Chap 12	6L	4
Unit-13	Frontiers: Touch and Proprioception, Smell and taste, Robotic interfaces and Brain-machine interfaces	Lavalle, Chap 13	3L	2
Text Books (MUST Know)	1. Steven Lavalle, "Virtual Reality", Cambridge Univerisity Press, (lavalle.pl/vr/book.html), 2020			
Reference Books (SHOULD Know)	1. Sherman W.R. and A B Craig, "Understanding Virtual Reality- Interface Application, and Design", Morgan Kaufmann, 2002. 2. Burdea G C and P Coffet, "Virtual Reality Technology", Second Edition, Wiley-IEEE presss, 2006.			
Laboratory Assignments/ Demonstrations				
1	Introduction to Unity 3D	Install Unity 3d and learn hands-on various features and functionalities	Unit 1	2
2	Virtual Reality App development using Unity3d	Develop a sample VR application and install it on target device for viewing	Unit 1-4	2
3	Augmented Reality App development using Unity3d and Vuforia	Develop a sample AR app and install it on target device for testing	Unit 1-4	2
4	AR App using Python, OpenCV and ARuco marker	Develop and Test python and OpenCV app to use ARUCO marker	Unit 10, 12	2
5	Virtual Tour app development and testing	Develop a VR Tour app and test it on target device	Unit 6,7	2
6	Points Cloud generation using Matterport for VR	Collect and install the images in Matterport to generate Point for testing	Unit 8	2

7	VR App: Case Study	Industry standard VR app is installed, tested and explored	Unit 1-12	2
8	AR App: Case Study	Industry standard AR App is installed, tested and explored	Units 1-12	2
9	Advanced VR App development using Unreal Engine/Unity 3d	An advanced app which involves scripting in C++/C# is developed using UnrealEnging or Unity3d	Units 1-12	2
10	Advanced AR App development using AR Tool kit	Develop and test the AR App	Units 1-12	2

Subject Code	**CE665A**
Subject Title	**Security Standards & Penetration Testing**
Credit	**04**
Type of Subject	-Core (MTech in CSE) -Professional Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	1. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 2. One Final Evaluation at the End of the Term **50 Marks** 3. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	Basic computer networking, operating systems and computer programming knowledge is required.
Dept	CSE
Course Objectives	This course examines the methods for securing information existing in different forms. This course will provide an introduction to the different technical and administrative aspects of Information Security and Assurance. Also, one cannot protect his information assets if he doesn't know how attackers think and what techniques attackers use to exploit systems. Hence, learning offensive security techniques like Ethical Hacking and penetration testing is becoming a need of future cyber security world. Objectives are: 1. To facilitate individual in gaining knowledge on information security management systems,.2. To facilitate individual in gaining knowledge on security standards like ISO-27001 standards, TCSEC, ITSEC, Secure coding etc. 3. To train individual to become competent information security professional by learning both theoretical as well as practical ethical hacking and penetration testing knowledge base
Course Outcomes	Bloom's Taxonomy: Level-1 Remember; Level-2 Understand; Level-3 Apply; Level-4 Analyze Level-5 Evaluate; Level-6 Create

	CO Title	Level	Descriptor
	CO1: Students will able to identify and apply basic concepts, terminology, theories, models and methods in the field of information security management field. (PO1, PO3, PSO1)	L1, L2	Remember, Understand
	CO2: Student will able to design policies for managing information security effectively adhering to ISO-27001 standards, TCSEC, ITSEC, Secure coding practices etc. (PO1,PO2, PO3, PSO1)	L3	Remember, Understand Analyse
	CO3: Student will learn to design, implement, integrate and manage various security countermeasures/tools/mechanisms/best practices and penetration testing through hands-on activities. (PO1, PO3, PSO1) attacks like Network Intrusion, DDOS, Malware attacks are carried out successfully by attackers. (PO1, PO2, PO3, PSO1, PSO2)	L3	Remember, Understand Analyse
	CO1, 03: End semester Exam	L4	Apply, Analyse

Syllabus Description

Basics & Preliminaries	Details	Books & References	Duration	COs
Unit-1	Introduction to Information security, Concepts, Threats, Attacks, and Assets, Security Functional Requirements, Countermeasures , Access Control Principles, Access Rights , Discretionary Access Control, Role - Based Access Control, Mandatory Access Control , Trusted Computing and Multilevel Security, Security Design Principles, Cryptographic Tools, Common Criteria for Information Technology Security Evaluation, Information security management systems (ISMS), ISO27000 and other security standards, Management responsibility, Responsibilities of Chief Information Security Officer (CISO)	Textbooks -1,2	12L	CO1
Unit-2	Security audits and assurance, Information Security Policy, Standards, and Practices, Asset Management, Human Resource Security, Security awareness training, Physical Security, Risk Management, Business continuity planning, Disaster Recovery planning, Penetration Testing Methodologies Security Assessments, Penetration Testing Methodologies, Penetration Testing Steps, Setting up own virtual ethical hacking lab for experimentation, Ethical Hacking and penetration Basics - Hacking terminology & attacks, Ethics, Legality.	Textbooks -2,3	12L	CO3
Unit-3	Phases – Reconnaissance, Scanning, Gaining access, Maintaining access, Covering tracks; Reconnaissance – Information gathering,Vulnerability research, Foot -printing, whois, DNS enumeration, Social Engineering, E – Mail Tracking, Scanning & Enumeration – Sniffing techniques & tools, Nmap, SYN, Stealth, XMAS, NULL, IDLE, and FIN Scans, detecting OS fingerprinting, banner grabbing, Null Sessions, SNMP/DHCP/DNS enumeration, Proxy Servers, Anonymizers,	Textbooks -2,3,4,5,6 References -1-7	12L	CO2

	HTTP Tunneling Techniques, IP Spoofing Techniques; Cryptographic Techniques, fuzz testing concepts			
Unit-4	Attacking System and Maintaining Access– Password/hashcracking, NetBIOS DoS Attacks, Password Cracking Countermeasures; Hiding FilesNTFS Stream Countermeasures, Steganography Technologies, Cover tracks and Erase Evidence, Disabling Auditing, Clearing the event Log, Malware attacks-Trojan, Backdoor, Viruses, Worms, DoS/DdoS; Attacks, Hacking and Penetration Testing Tools like Kali Linux, Metasploit ,Pen-Test Deliverables	Textbooks -4-6, / References -1-7	12L	CO2
	LAB/ Assignments/Student Presentations [2T/P per week		02L/ Week	CO4

Text Books (MUST Know)	7. Michael E Whitman, Herbert J Mattord, "Principles of Information Security", Course Technology, 3rd Edition, 2008. 8. Dhavale, S. V. (2019). Constructing an Ethical Hacking Knowledge Base for Threat Awareness and Prevention (pp. 1-305). Hershey, PA: IGI Global. 9. Stuart McClure, Joel Scambray, George Kurtz, "Hacking Exposed:n/w sec secrets and solutions", Mcgraw Hill, 2012
Reference Books (SHOULD Know)	8. Various Security Standards - ISO 27000 series published by ISO. 9. Department of Defense Standard, Department of Defense, "Trusted Computer System Evaluation Criteria", Orange Book. 10. Dieter Gollmann, "Computer Security", John Wiley and Sons, Inc., 3rd edition, 2011 11. David Kennedy, Jim O'Gorman, Devon Kearns, and MatiAharoni, "Metasploitpentest guide",No starch Press, san Francisco, 2011 12. Bastian ballman, "Understanding n/w hacks:attack and defense with python", Springer,2012 13. Rich Annings, HimanshuDwivedi, Zane Lackey, "Hacking Exponsed Web 2.0", Tata Mcgraw hill Edition 14. Research paper for study (if any) - White papers on multimedia from IEEE/ACM/Elsevier/Spinger/IBM/EC-Council sources 15. Krutz, R. L. & Vines, R. D., "The CISSP and CAP Prep Guide", Platinum Edition, New York, Wiley Publishing., 2006. 16. Nina Godbole, "Information Systems Security: Security Management, Metrics, Frameworks and Best Practices", Wiley India Pvt Ltd, 2012. 17. William Stallings and Lawrie Brown, "Computer Security: Principles and Practice", 2nd edition, Pearson, 2012.

Laboratory Assignments/ Demonstrations

1	Study Windows Essential Tools-Part 1	Unit -1	02 hours	CO1, CO2,CO3, & CO4
2	Study Windows Essential Tools-Part 2	Unit -1	02 hours	CO1, CO3, & CO4
3	Study Sysinternals utilities to manage, diagnose, troubleshoot, and monitor a Microsoft Windows environment	Unit -2	02 hours	CO2, CO3, & CO4
4	Study passive information gathering tools.	Unit -3	02 hours	CO1, CO3, & CO4
5	Write Security Policy Document	Unit -3	04	CO1, & CO4

			hours	
6	Case study: LDRA and Parasoft tools	Unit -3	02 hours	CO2, & CO3
7	Kali Linux Attacks – Part1	Unit -3	02 hours	CO3, & CO4
8	Kali Linux Attacks – Part2	Unit -4	04 hours	CO2, & CO3
9	SSPT Practice Test -1Quiz	Unit -4	02 hours	CO2, & CO4
10	Apply data mining tools for cyber security related data analysis	Unit -4	04 hours	CO1,CO2, CO3, & CO4

Subject Code	**CS-611**			
Subject title	**Digital Forensics**			
Credit	**04**			
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/weekTotal Contact hours 05 per week.			
Evaluation Pattern	1. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 2. One Final Evaluation at the End of the Term **50 Marks** 3. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**			
Total Marks	100 Marks			
Prerequisite	Knowledge of OS, Assembly Languages like Python, Number System and their Conversions, Internal Structure of CD/DVD.			
Course Outcomes	CO1: Students will be able to understand the standard procedures of Digital Forensics required for Cyber Crime Investigation. CO2 : Students will be able to apply proper commands and procedures required for digital investigation. CO3: Students can practically demonstrate or articulate the suspicious activity/artifacts extraction w.r.t. from the digital evidence. CO4: Students will be able to solve the real-time case-studies available on benchmarked repositories			
Syllabus Details	**Details**	**Text books/Reference books**	**No. of Hrs**	**Cos**
Unit 1	Introduction to digital forensics Stages of Forensic: acquisition or imaging of exhibits, analysis and reporting standards Introduction to Computer Forensics: Digital Devices with rudimentary computing power Acquisition or imaging of Onboard Memory and Static	Text Book1, R3	12	CO1, CO4

	Memory Introduction to legal issues, Analysis and Reporting Standards,Online and Live Forensics			
Unit 2	Forensic study of database and their metadata, database contents, log-files for creating timeline or recover relevant information	Text Book3	12	CO3, CO4
Unit 3	MFT & Registry Hives Extraction from Windows OS through Tools and Scripts Data Carving Using Open Source Tools,Data Recovery and Secure deletion on Storage media. Evidence or Intrusion detection from internet logs, monitoring and analysis of network traffic.Internet of Things	Text Book2, R1	12	CO2, CO4
Unit 4	Drone Forensics: Internal and External Memory Artifacts Analysis of DJI Drone Models, Study of Various Drone-Components and their Artifacts, Fly-Path Reconstruction, Directory Analysis, Telemetry Data Recovery from Internal and External Memory of particular Drone Model	Text Book2, R2	12	CO2, CO4

Text Book:

1. Kanellis, Panagiotis, "Digital Crime and Forensic Science in Cyberspace", IGI Publishing", ISBN 1591408733.
2. Marshell, Angus M. (2008), "Digital Forensics: Digital Evidence in Criminal Investigation", Wiley-Blackwell, ISBN 0470517751.
3 Brain Carrier, "File System Forensics Analysis", Addison-Wesley Professional, 1st Edition, 2005

Reference Books:

1. Chris Prosise, Kevin Mandia " Incident Response & Computer Forensics", McGraw-Hill, 2nd Edition, 2003.
2. Rick Ayers, Sam Brothers, Wayne Jansen, "Guidelines on Mobile Device Forensics", NIST, US Dept. of Commerce, Revision 1, 2014
3. Pavan Duggal, "Cyberlaw–The Indian Perspective", 2009 Edition

Lab Assignments

Name of Experiments	Units	Duration (Hrs)	Co's
1. Perform Imaging and Analysis of Non-Volatile Memory using Open Source Tools in the absence of Write-Blockers.	I	02	CO1, CO4
2. Perform Imaging and Analysis of Non-Volatile Memory using EnCase/Other Open Source Tools With and Without Write Blockers.	I	02	CO1, CO4
3. Explore the Phases of Ethical Hacking in terms of implementing some attack.	I	02	CO1, CO4
4. Perform Imaging and Analysis of Volatile Memory using EnCase/Other Open Source Tools	I	02	CO1, CO4
5. MFT & Registry Hives Extraction from Windows OS through Tools and Scripts.	II	02	CO3, CO4
6. Recovering Deleted File from the File System	II	02	CO3, CO4
7. SystemHiding Data into Slack Space.	II	02	CO3, CO4
8. Data Recovery and Secure deletion on Storage media.	III	02	CO2, CO4

9. Data Carving Using Open Source Tools	III	02	CO2, CO4
10. Information gathering and network traffic analysis using TCP DUMP and WIN DUMP	III	02	CO2, CO4
11. Attacks and Forensics using IoT devices	IV	02	CO3, CO4
12. Social Network Artifacts Extraction and Analysis.	IV	02	CO3, CO4

Subject Code	**CS-612**	
Subject Title	**Reverse Engineering & Malware Analysis**	
Credit	**04**	
Type of Sub	- Open Elective for All Engineering and Science disciplines	
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.	
Evaluation Pattern	34. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 35. One Final Evaluation at the End of the Term **50 Marks** 36. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**	
Total Marks	100 Marks	
Prerequisite	OS fundamentals, Basics of Assembly language programming.	
Dept	CSE	
Course Objective	The course introduces reverse engineering techniques and further examines the use of reversing for detecting, analyzing, and eradicating malware. It involves: 1 Learning low level details of binary files and applying the reverse engineering techniques and tools to analyse any binary file without documentation. 2 Techniques to prevent binary file from reversing 3 Common vulnerabilities and protections in binary 4 Static and dynamic malware analysis	
Course Outcomes	On completion of this course, the students should be able to	
	CO Title	**Level**
	CO1 - Reverse engineer a binary executable file in an understandable form.	Level 2,3,4
	CO2 - Detect the vulnerabilities in the executable code.	Level 3/4/5
	CO3 - Identify the different types of malware analysis methods to recognize the binary with evasive, anti-reversing mechanism.	Level 4/5
	CO4 - Perform code analysis and recognize common malware characteristics. Setup an environment for malware analysis and perform runtime analysis. Understand and trace process execution on a system.	Level 4/5
CO-PO: Course Outcome and Program Outcome Evaluation Metrics		

	PO1	PO2	PO3	PSO1	PSO2
CO1	-	-	Y	Y	-
CO2	Y	-	Y	Y	-
CO3	Y	-	Y	Y	Y
CO4	Y	Y	Y	Y	Y

Syllabus Description

Unit	Topics	Text Book	Duration	COs
Unit-1	Introduction to reverse engineering; Low level software perspective; Windows OS fundamentals; Compilers, Execution Environments; Assembly language primer; Executable file formats; Calling Conventions; Offline code analysis; Reversing tools, Disassemblers, Debuggers, Decompilers, System monitoring tools;	Text Book-1, Ch-1	16L	CO1, CO2, PO1, PO3, PSO1
Unit-2	Static or offline reversing of program binaries Dynamic reverse engineering; Debugging binary cod	Text Book-1, Ch-2, 3	10L	CO2, PO1, PO3, PSO1
Unit-3	Anti-reversing techniques, Breaking protections Reversing '.NET', De-compilation Software vulnerabilities – buffer overflow, integer overflow, vulnerabilities exploitation, mitigation; Return oriented programming;	Text Book-1, Ch-4	12L	CO2, CO3; PO1, PO3, PSO1, PSO2
Unit-4	Introduction to malware Reversing malware – Static & Dynamic malware analysis techniques Packers & compression, Sandboxing executables& runtime analysis; Fileless Malware; Malware classification STUDENT PRESENTATION & INTERACTIVE SESSIONs	Text Book-1, Ch-4, 5	10L+8T	CO3, CO4; PO1, PO2, PO3, PSO1, PSO2
Text Books (MUST Know)	1. Eldad Eilam, "Reversing: Secrets of Reverse Engineering", Wiley publishing, 2005 2. Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware, by Abhijit Mohanta (Author), Anoop Saldanha, September 2020			
Reference Books (SHOULD Know)	1. Michael Ligh, Steven Adair, "Malware Analysts's cookbook & DVD", Wiley publishing 2. Michael Sikorski and Andrew Honig, Practical Malware Analysis, No Starch Press, 2012. 3. Abhishek Singh, "Identifying Malicious Code through Reverse Engineering", Springer Publcations, 2009. ISBN No – 978-0-387-09824-1 4. Erik Buchanan, Ryan Roemer, HovavShacham, and Stefan Savage. 2008. "When good instructions go bad: generalizing return-oriented programming to RISC."			

Laboratory Assignments/ Demonstrations-

1	To explore the components of executable file in Linux and Windows.	Unit-1		CO1
2	To Debug an executable to reverse DLL using Ollydbg and IDA Pro	Unit-1		CO2
3	Dll injection	Unit-2		C03
4	IAT extraction	Unit 1 & 2		CO3
5	Usage of system monitoring tools	Unit 1,2,3,4		CO2
6	Packing and analysis of executable files	Unit 3,4		CO3
7	Find vulnerability in executable code	Unit 2,3		CO3
8	Advanced Static Analysis of Malware samples	Unit 4		CO4
9	Advanced Runtime Analysis of Malware samples	Unit 4		CO4
10	To explore the components of executable file in Linux and Windows.	Unit 2,3		CO2
11	Mini Project Statements: Hooking Detection, Keylogger Implementation and Detection, Heuristic rules for Malware Detection, Stack Smashing Attack / ROP Attack, Malware analysis & Report presentation	Unit 1,2,3,4		CO1, CO2, CO3, CO4

Subject Code	**CE 70G**
Subject title	**Blockchain Technology**
Credit	**04**
Type of Sub	- Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	37. Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** 38. One Final Evaluation at the End of the Term **50 Marks** 39. Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	Expertise in Programming, Basic Knowledge of Computer Security, Cryptography, Networking.
Dept	CSE
Course Objective	Blockchain is an emerging technology platform for developing decentralized applications and data storage, The basic tenet of this platform is that it allows one to create a distributed and replicated ledger of events, transactions, and data generated through various IT processes with strong cryptographic guarantees of tamper resistance, immutability, and verifiability. The technology itself holds much more promise in various areas such as time stamping, logging of critical events in a system, recording of transactions, trustworthy e-governance etc. Many researchers are working on many such use cases such as decentralized public key infrastructure, self-sovereign identity management, registry maintenance, health record management, decentralized authentication, decentralized DNS, etc. Considering the need to disseminate the emerging concepts for students, we

	proposed a new course on blockchain technology, includes the fundamental design and architectural primitives of Blockchain, the system and the security aspects, along with various use cases from different application domains
Syllabus Description	
Unit-1	Basic Cryptographic primitives used in Blockchain – Secure, Collison-resistant hash functions, digital signature, public key cryptosystems, zero-knowledge proof systems
Unit-2	Basic Distributed System concepts – distributed consensus and atomic broadcast, Byzantine fault-tolerant consensus methods.
Unit-3	Basic Blockchain – concepts to Bitcoin and contemporary proof-of-work based consensus mechanisms, operations of Bitcoin blockchain, crypto-currency as application of blockchain technology
Unit-4	Ethereum Blockchain: Samrt Contract, Introduction to Solidity Language, Proof of stake, Ethereum Network
Unit-5	Hyperledger fabric platform- Decomposing the consensus process , Hyperledger fabric components, Chaincode Design and Implementation Hyperledger Fabric
Unit-6	IoTA : Formation of Tangle, Cumulative weight, Consensus in IoTA, Double Spending Attack.
Unit-7	Beyond Cryptocurrency – applications of blockchain in cyber security, integrity of information, E-Governance and other contract enforcement mechanisms
Unit-8	Security and Research Aspects
Reference Books (SHOULD Know)	1. Bitcoin and Cryptocurrency Technologies by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, Princeton University Press 2. "S. Shukla, M. Dhawan, S. Sharma, S. Venkatesan, 'Blockchain Technology: Cryptocurrency and Applications', Oxford University Press. 3. Josh Thompson, 'Blockchain: The Blockchain for Beginnings, Guild to Blockchain Technology and Blockchain Programming', Create Space Independent Publishing Platform.

Subject Code	**CE 66A**
Subject Title	**Algorithmic Cryptanalysis**
Credit	**04**
Course Objectives	This course discusses cryptanalysis from basics to advanced application from algorithmic point of view. After completion of the course, the students should be able to identify and apply the suitable algorithm for more sophisticated cryptographic applications, including LFSR-based stream ciphers and index calculus methods. The students should be able to observe the advancements in

	current computer architectures and its impact on implementation aspects of cryptanalysis methods.
Prerequisite	Preferred if subjects related to cryptography and algorithms are studied in graduation or semester-I.
Pre-requisite training	One week training on basics of Cryptography & algorithms.
Syllabus	
UNIT-1	Preliminaries, Defining security in cryptography, Elementary Number Theory and Algebra, Evolution in Computing Devices, Evolution in Communication Media, Evolving Programming Environments, Three Generic Forms of Cryptanalysis: Cipher text only, Known cipher text/plain text pairs, and Chosen plain text or chosen cipher text.
UNIT-2	General Approaches to Cryptanalysis – (i) based on properties on encryption algorithms & (ii) brute force, Linear Algebra, Sieve Algorithms, Brute Force Cryptanalysis, The Birthday Paradox: Sorting or Not? Birthday-Based Algorithms for Functions, Algorithmic complexities & computational costs.
UNIT-3	Birthday Attacks through Quadrisection, Fourier and Hadamard–Walsh Transforms, Lattice Reduction, Polynomial Systems and Gröbner Bases Computations; Study of protocols for cryptanalysis**.**
UNIT-4	Attacks on Stream Ciphers, Lattice-Based Cryptanalysis, Elliptic Curves and Pairings, Index Calculus Algorithms
Text Book	Algorithmic Cryptanalysis, by Antoine Joux, 2010
Reference Books	1. Cryptanalysis: A Study of Ciphers and Their Solution (Dover Brain Games), by Helen F. Gaines , 1956 2. Cryptanalysis of Number Theoretic Ciphers, By Samuel S. Wagstaff, Jr., 2002.

CE699 Internet of Things

Syllabus:

Unit I Introduction to Internet of Things, Definition and Characteristics of IoT, Physical Design of IoT, IoT Protocols, IoT communication models, IoT Communication APIs

Unit II IoTenablingTechnologies, Wireless Sensor Networks, Cloud Computing, Big data analytics,

Communication protocols, Embedded Systems, IoT Levels and Deployment Templates, Domain Specific IoTs: Home, City, Environment, Energy, Retail, Logistics, Agriculture, Industry, health and Lifestyle

Unit III 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 IV IoT physical end devices & end points, IoT Physical Servers & Cloud offerings,Software environments, NEO, Security

Text /Reference Books:

5. "Internet of Things: A Hands-on Approach", by ArshdeepBahga and Vijay Madisetti (Universities Press), 2014
6. "The Internet of Things: Enabling Technologies, Platforms, and Use Cases", by PethuruRaj and Anupama C. Raman (CRC Press)
7. "Designing the internet of things", McEwen, Adrian, and Hakim Cassimally. John Wiley& Sons, 2013.
8. Research Papers discussed in the classroom discussions.

CE633 Pattern Recognition

Syllabus:

Unit I: Basics of Probability, Random Processes and Linear Algebra (recap): Probability: independence of events, conditional and joint probability, Bayes theorem Random Processes: Stationary and non-stationary processes, Expectation, Autocorrelation, Cross-Correlation, spectra.

Unit II: Linear Algebra: Inner product, outer product, inverses, eigen values, eigen vectors,singular values, singular vectors.

Unit III: Bayes Decision Theory : Minimum-error-rate classification. Classifiers, Discriminant functions, Decision surfaces.Normal density and discriminant functions. Discrete features.

Unit IV: Parameter Estimation Methods : Maximum-Likelihood estimation :Gaussian case. Maximum a Posteriori estimation. Bayesian estimation: Gaussian case. Unsupervised learning and clustering - Criterion functions for clustering. Algorithms for clustering: K- Means, Hierarchical and other methods. Cluster validation. Gaussian mixture models, Expectation-Maximization method for parameter estimation. Maximum entropy estimation.Sequential Pattern Recognition. Hidden Markov Models (HMMs). Discrete HMMs. Continuous HMMs. Nonparametric techniques for density estimation.Parzen- window method.K-Nearest Neighbour method.

Unit V: Dimensionality reduction: Principal component analysis - it relationship to eigen analysis. Fisher discriminant analysis - Generalised eigen analysis. Eigen

vectors/Singular vectors as dictionaries. Factor Analysis, Total variability space - a dictionary learning methods.Non negative matrix factorisation - a dictionary learning method.

Unit VI: Linear discriminant functions : Gradient descent procedures, Perceptron, Support vector machines - a brief introduction.

Unit VII: Artificial neural networks: Multilayer perceptron - feedforwark neural network. A brief introduction to deep neural networks, convolutional neural networks, recurrent neural networks.

Unit VIII: Non-metric methods for pattern classification : Non-numeric data or nominal data. Decision trees: Classification and Regression Trees (CART).

Text /Reference Books:

1. R.O.Duda, P.E.Hart and D.G.Stork, Pattern Classification, John Wiley, 2001
2. S.Theodoridis and K.Koutroumbas, Pattern Recognition, 4th Ed., Academic Press, 2009
3. C.M.Bishop, Pattern Recognition and Machine Learning, Springer, 2006

CE691 SECURE WIRELESS SENSOR NETWORKS

Background: Wireless Sensor networks (WSN) is an emerging technology and have great potential to be employed in critical situations like battlefields and commercial applications such as building, traffic surveillance, habitat monitoring and smart homes and many more scenarios. One of the major challenges wireless sensor networks face today is security. While the deployment of sensor nodes in an unattended environment makes the networks vulnerable to a variety of potential attacks, the inherent power and memory limitations of sensor nodes makes conventional security solutions unfeasible. The sensing technology combined with processing power and wireless communication makes it profitable for being exploited in great quantity in future. The wireless communication technology also acquires various types of security threats.

Objective: To meet End-User, Network-Administrator and Network-Designer perspectives

Prerequisite: Computer Networks Fundamentals, Programming,

Syllabus:

Unit I: Introduction, WSN Resources & constraints, Relevance to IoTs, Relevance to Cyber-Physical Systems, Relevance to Network Centric Operations, Relevance to Data Stream Management Systems, Relevance to the increasing demand of high performance computations, SCADA, battle sensor.

Unit II**:** WSN Network Architecture, MAC Layer protocols, Naming and Addressing, Synchronization, Location & positioning, Topology control, Connected Dominating Sets, Routing Protocols, Data-Centric & Content-based networking, Data-Centric querying, WSNs versus IoTs

Unit III: Vulnerabilities, threats, attacks & safeguards in WSN, key distribution methods & protocols, multi-party computations inclusion, RF-Id communications, open source hardware concept, Security goals for WSNs, Attacks on WSNs: Passive & Active Attacks, Security Mechanisms, Security Models

for WSNs, Challenges in WSNs: with respect to wireless medium, resource scarcity, ad-hoc deployments, hostile environments, immense scale, etc. Application oriented: Secure Wireless Networks.

Text Book:

1. FUNDAMENTALS OF WIRELESS SENSOR NETWORKS: THEORY AND PRACTICE, Authors: Waltenegus Dargie, Technical University of Dresden, Germany, Christian Poellabauer, University of Notre Dame, USA, Wiley, First Edition, 2010

Research Paper References:

20. Ian F. Akykildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, —A Survey on Sensor Networks‖, IEEE Communication Magazine, year 2002.
21. Culler, D. E and Hong, W., —Wireless Sensor Networks‖, Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.
22. Adrian Perrig, John Stankovic, David Wagner, —Security in Wireless Sensor Networks‖ Communications of the ACM, Page53-57, 2004
23. Chris Karlof, David Wagner, —Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures‖, AdHoc Networks (elsevier), Page: 299-302, year 2003
24. Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, —Security in Wireless Sensor Networks: Issues and Challenges‖, International conference on Advanced Computing Technologies, Page1043-1045, year 2006
25. John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, —Wireless Sensor Network Security: A Survey‖, Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10-15, year 2006
26. Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong, —Security in wireless sensor networks: issues and challenges‖ Advanced Communication Technology (ICACT), Page(s):6, year 2006
27. Tahir Naeem, Kok-Keong Loo, Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks, International Journal of Digital Content Technology and its Applications, Page 89-90 Volume 3, Number 1, year 2009
28. Undercoffer, J., Avancha, S., Joshi, A. and Pinkston, J. —Security for sensor networks‖. In Proceedings of the CADIP Research Symposium, University of Maryland, Baltimore County, USA, year 2002 http://www.cs.sfu.ca/~angiez/personal/paper/sensor-ids.pdf
29. Zia, T.; Zomaya, A., —Security Issues in Wireless Sensor Networks‖, Systems and Networks Communications (ICSNC) Page(s):40 – 40, year 2006
30. Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou, Sensor Network Security: A Survey, IEEE Communications Surveys & Tutorials, vol. 11, no. 2,page(s): 52-62, year 2009
31. D. Djenouri, L. Khelladi, and N. Badache, —A Survey of Security Issues in Mobile ad hoc and Sensor Networks,‖ IEEE Commun. Surveys Tutorials, vol. 7, pp. 2–28, year 2005.
32. S. Schmidt, H. Krahn, S. Fischer, and D. Watjen, —A Security Architecture for Mobile Wireless Sensor Networks,‖ in Proc. 1st European Workshop Security Ad-Hoc Sensor Networks (ESAS), 2004.
33. Y. Wang, G. Attebury, and B. Ramamurthy, —A Survey of Security Issues in Wireless Sensor Networks,‖ IEEE Commun. Surveys Tutorials, vol. 8, pp. 2–23, year 2006.
34. Yun Zhou, Yuguang Fang, Yanchao Zhang, Securing Wireless Sensor Networks: A Survey, IEEE Communications Surveys & Tutorials, year 2008
35. Xiuli Ren, Security Methods for Wireless Sensor Networks, Proceedings of the 2006 IEEE International Conference on Mechatronics and Automation , Page: 1925 ,year 2006
36. R.Roman, J. Zhou, and J. Lopez, —On the security of wireless sensor networks,‖ in International

Conference on Computational Science and Its Applications – ICCSA 2005, May 9-12 2005, vol. 3482 of Lecture Notes in Computer Science, (Singapore), pp. 681– 690, Springer Verlag, Heidelberg, D-69121, Germany, 2005.
37. N. Sastry and D. Wagner, —Security considerations for ieee 802.15.4 networks,‖ in Proceedings of the 2004 ACM workshop on Wireless security, pp. 32–42, Philadelphia, PA, USA: ACM Press, 2004.
38. WSN Security Models: Refer 4 papers: Paper 1: Wireless sensor network security model using zero knowledge protocol, ICC 2011; Paper 2. An energy efficient link-layer security protocol for wireless sensor networks, EIT 2007; Paper 3. Toward resilient security in wireless sensor networks, MobiHoc 2005; Paper 4. TinySec: a link layer security architecture for wireless sensor networks, SenSys 2004.

Tutorials:

k. Routing techniques: Overview of Proactive and reactive routing protocols, significance of *a hop* in adhoc networks
l. Flooding, Gossiping, Zonal Routing Protocols ZRP, Hybrid Routing, TTL significance with respect to routing protocols
m. Impact of hardware and software on Battery Performances/Utilisation
n. IEEE 802.15.4: A study, Features, Types of Devices FFD (PAN coordinators, Coordinators), RFDs Reduced Function Devices, Network Setup process & parameters in Consideration, Programming Strategies to suit the standards, MAC and PHY structure
o. Demo 1: Controlling DIOs. Demonstrate the usage of DIO using LEDs. Learning how to handle data sampling period.
p. Demo 2. Reading data from a single IoT device. Interpretation of data.
q. Demo 3: Create a broadcast wireless network and capture the traffic generated by the participating nodes.
r. Demo 4. Creating a multi-hop network using MBR routing.
s. Understanding MBR & LBR (MAC Based Routing and LBR Level-Based Routing)
t. Understanding exiting API, Libraries & its association with pre-existing demonstration codes.

Subject Code	**CE694**
Subject Title	**Big Data Analysis & Algorithms**
Credit	**04**
Type of Subject	-Core (MTech in CSE) -Open Elective for All Engineering and Science disciplines
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	• Continuous Evaluations: Three Monthly Test (10 Marks Each) **30 Marks** • One Final Evaluation at the End of the Term **50 Marks** • Lab Assignments/Mini-Project and Term Work Evaluations: **20 Marks**
Total Marks	100 Marks
Prerequisite	None.

	First 10 hours will be devoted for Prerequisite learnings related to basics of Databases (04 hours), Computer Networks (02 Hours), Operating System (02 Hours), Trends in evolutions of Compute-Devices (02 Hours)
About the Course	I. The use of Big Data is becoming a crucial way for leading companies to outperform their peers. In most industries, established competitors and new entrants alike will leverage data-driven strategies to innovate, compete, and capture value. Early adopters of Big Data are using data from sensors embedded in products from children's toys to industrial goods to determine how these products are actually used in the real world. Such knowledge then informs the creation of new service offerings and the design of future products. Big Data will help to create new growth opportunities and entirely new categories of companies. With everything going digital, data is pouring in from all kinds of sources imaginable. Organisations are getting inundated with terabytes and petabytes of data in different formats from sources like operational and transactional systems, customer service points, and mobile and web media. The problem of such huge data is storage and with no proper utilisation of the data, collecting and storing is a waste of resource. Earlier it had been difficult to process such data without relevant technology. Big data analytics is becoming an integral part of organisations who want to grow in this age of innovation and is being done by most of the big companies. There is huge scope of big data analytics professionals as this is going to be an essential part of companies in the future. II. **The Need:** (a) Cyber-Security Perspective: As the complexity of IT networks has grown, the inventiveness and sophistication of cyber security threats and attacks has grown just as quickly. As malware attacks increase in volume and complexity, it's becoming more difficult for traditional analytic tooling and infrastructure to keep up thanks to the Data volume, For example, every day at Sophos Labs, over 300,000 new potentially malicious files that require analysis are reported. Scalability: SQL-based tooling and infrastructure doesn't scale well and is costly to maintain. Big Data Analytics is a Path Forward to Cyber Security. (b) AI / Intelligent Systems Perspective: Centre for Big Data Analytics and Intelligent Systems focuses on the theory development, novel techniques and smart solutions of big data analytics in broad domains, along with theories and techniques of building computer systems, which capture the intelligent behaviours in complex environments. AI dwells on Big Data. (c) Multi-Disciplinary Course useful to any engineering discipline who use a computer.
Course Outcomes & Objective	III. To meet end-user, administrator & system designer perspectives, develop skill sets to be resourceful in building and handling knowledge & information systems. Enhance analytical capabilities to evaluate a domain specific and technical area. Multi-Disciplinary Course useful to any engineering discipline who use computer. IV. To educate the stakeholders on the growth of importance of information security. Along with personal utilization of systems, the privacy matters in the government, enterprise arenas. The study will significantly broaden the scope of individuals who must be aware of relevant issues as part of their work.
OBE Course Outcomes	Bloom's Taxonomy: Level-1 Remember; Level-2 Understand; Level-3 Apply; Level-4 Analyze Level-5 Evaluate; Level-6 Create

	CO Title	Level	Descriptor	Expected Outcome
	CO1: Student will be able to examine and identify Data Models for various applications	L1, L2	Remember, Understand Learn,	20%
	CO2: Student will be able to apply data abstraction & normalisation techniques to handle volume and veracity	L3, L4	Apply, Analyse	20%
	CO3: Student will be able to analyze & apply multi-dimensional data models for complex scenarios	L4, L5	Analyse, Evaluate	20%
	CO4: Student will be able to evaluate the system requirements and propose solutions using various data models to cater special application requirements & to form a base to apply Data Mining & AIML techniques.	L5, L6	Evaluate, Create	40%

CO-PO : Course Outcome and Program Outcome Evaluation Metrics

	PO1	PO2	PO3	PSO1	PSO2
CO1	Y			Y	Y
CO2	Y	Y		Y	Y
CO3		Y	Y		Y
CO4			Y		Y

Summary of the Course OutCome	At the end of the course, a student will understand the concepts of data models. Use data models. Evaluate requirements to address emerging areas of data handling with the growing needs. Broadly defined roles. Knowledge of enabling systems. Conducive environment building for data analysts. Data engineering to handle the data at public and private sectors while complying with the data policies to be professionals who understand structured and unstructured data and the challenges to handle them.

Syllabus Description

Basics & Preliminaries	Types of Data Models, Role of Basic and Advanced Data Structures in Data Models, Basic Dictionary Data Types; Algorithms and basics of analysis, OS & Algorithms in Parallel Environments. Protocols of Computer Networks preliminaries, Concerns for Data Security and Privacy	Cormen et al, Horowitz & Sahani, Bipin Desai, Korth et al. Kurose Ross	10 Hours	CO, PO1
Unit-1	Introduction to big data analysis: Evolution of data, data streams, database models, graph data, normalizations, structured & unstructured data,	Text Book-1, Ch-1	08 Hours	CO1, CO2, PO1

Unit-2	Architectures, Adoption, Frameworks that enable big data analytics, Multi-Dimensional Data Models, Data cube Computations	Text Book-1, Ch-2, 3	04 Hours	CO1, PO1
Unit-3	Data Preprocessing, Data Warehousing OLTPS, OLAPS, Data Warehouse Architectures, Big Data Mining Frequent Patterns, Big Data Associations & Correlations, Classifications & Predictions, Clustering Techniques & Analysis, Mining Data Streams, Graph Mining, Mining Spatial & Temporal Objects, Predictive Analysis, Ad Hoc Queries, Web Analytics	Text Book-1, Ch-4	06 Hours	CO1 CO2, PO1
Unit-4	Algorithms for SISD, SIMD environments, Linked Big Data Analysis – Graph Computing and Network Science, Big Data Visualization, Big Data Mobile Applications, Large-Scale Machine Learning, Big Data Analytics on Specific Processors, Hardware and Cluster Platforms for Big Data Analytics, Big Data Next Challenges – IoT, Cognition, and Beyond	Text Book-1, Ch-4, 5	06 Hours	CO3, PO2
Unit-5	Big Data Storage & Processing Concepts Relational database technology, Parallel and Distributed Processing capabilities, Clouds, MapReduce Framework	Text Book-1, Ch 5,6,7,8	06 Hours	CO3, PO2, PO3
Unit-6	Database Auditing Models Technical Audit Environment, Process, Objectives, Classification Types, Incidence Reports, Level of escalations. Application Data Audit: DML Action Audit; Triggers; Fine-Grained Auditing FGA; Application Errors; PL-SQL Environments, Audit DB Activities	Weblink References	06 Hours	CO4, PO2, PO3
Unit-7	Big data analytics tools, HDFS, NOSQL, SQL environments Project Cases Big data, Big Data Security: Online Databases; CSV files to Structured Environments, SCADA, IoTs,	Text Book-1, Ch-8	06 Hours	CO1, CO4, PO1, PO3
Text Books (MUST Know)	Text Book 1 : Big Data Fundamentals: Concepts, Drivers & Techniques (Prentice Hall Service Technology) Paperback – Import, 5 Jan 2016 by Thomas Erl (Author), Wajid Khattak (Author), Paul Buhler (Author), Publisher: Prentice Hall (5 January 2016), 240 pages , ISBN-10: 0134291077 , ISBN-13: 978-0134291079		Must Know.	

	Text Book-2: Big Data: Concepts, Technology, and Architecture, Balamurugan Balusamy, Nandhini Abirami R, Seifedine Kadry, Amir H. Gandomi, Wiley Publications, ISBN: 978-1-119-70185- 9 March 2021		
Reference Books (SHOULD Know)	Reference Book-1 Data Mining, Jiawei Han & Micheline Kamber, 2nd edition, Elsevier, 2006	Should Know.	
Consortium, e-books and Web Link references (SHOULD/ Could Know)	1. https://iveybusinessjournal.com/publication/why-big-data-is-the-new-competitive-advantage/ 2. https://www.datameer.com/company/datameer-blog/challenges-to-cyber-security-and-how-big-data-analytics-can-help/ 3. https://www.iss.nus.edu.sg/executive-education/discipline/detail/analytics-and-intelligent-systems 4. W3.org 5. Meity.gov.in 6. SIGSAC SIGSEC acm.org 7. Isca-speech.org 8. Issa.org 9. Oracle.com/database/ 10. Thelawreviews.co.uk 11. Data Security Council of India (DSCI) 12. prsindia.org 13. iso.org ISO/IEC 27000/27001/27002	Should and Could Know.	

Laboratory Assignments/ Demonstrations

LAB Assignments	*Each student will work on unique case study. Will require approval of the same at the beginning. Report submission is essential for each Lab Assignment.			
1	Describe the Use Case*. Model the case study. Abstract. Apply & implement DDL.	Unit-1	02 hours	CO1
2	Data Manipulation Language (DML) and Data Control Language (DCL)	Unit-2	02 hours	CO2
3	Apply, analyse and evaluate ACID Properties. High level language extensions with cursors. High level language extension with Triggers.	Unit-3 & 4	02 hours	C03
4	Implement and apply Multi-dimensional DBs. Implement three basic operations: Perform Diagnostic Analysis	Unit 4 & 5	02 hours	CO3
5	Implement and apply Multi-dimensional DBs. Implement operations to observe 'what-if' analysis: Perform Predictive Analysis	Unit 4 & 5	02 hours	CO4
6	Create use case environment, Implement & Perform Data Flow wrt Application/Domain Control	Unit 6	02 hours	CO4
7	Create use case environment, implement & perform Inter-environment mappings and data pre-processing to apply to AIML model.	Unit 6	02 hours	CO4