CURRICULUM AND DETAILED SYLLABI

FOR

M.E. COMPUTER SCIENCE AND INFORMATION SECURITY DEGREE PROGRAMME

FOR THE STUDENTS ADMITTED IN THE

ACADEMIC YEAR 2018-19 ONWARDS

THIAGARAJAR COLLEGE OF ENGINEERING

(A Government Aided ISO 9001:2008 certified Autonomous Institution affiliated to Anna University)

MADURAI – 625 015, TAMILNADU

Phone: 0452 – 2482240, 41
Fax: 0452 2483427
Web: www.tce.edu

THIAGARAJAR COLLEGE OF ENGINEERING
DEPARTMENT OF INFORMATION TECHNOLOGY

VISION

Evolve into a **Centre of Excellence for Education and Research** in Information Technology.

MISSION

- Attaining academic excellence through well designed curriculum adaptable to dynamic technological needs, competent faculty and innovative teaching-learning process.
- Promoting collaborative research through special interest groups, state of the art research labs Industry Institute interactions
- Facilitating value added courses to produce highly competent and socially conscious information technology professionals and entrepreneurs.

PROGRAM EDUCATIONAL OBJECTIVES

Graduates of the programme will

PEO 1 Contribute effectively to serve the society through information security enabled solutions and products adhering to professional ethics and cyber laws.

PEO 2 Articulate fundamental concepts, design underpinnings of information security, and research findings to train professionals or to educate engineering students.

PEO 3 Ppursue academic research in Information Security and contribute significantly in the field of Computer science.

PEO 4 Engage in lifelong learning to adapt to changing technological needs for career advancement.

PROGRAM OUTCOMES

PO1 Scholarship of Knowledge

Acquire in-depth knowledge of specific discipline or professional area, including wider and global perspective, with an ability to discriminate, evaluate, analyse and synthesize existing and new knowledge, and integration of the same for enhancement of knowledge.

PO2 Critical Thinking

Analyse complex engineering problems critically, apply independent judgment for synthesizing information to make intellectual and/or creative advances for conducting research in a wider theoretical, practical and policy context.

PO3 Problem Solving

Think laterally and originally, conceptualize and solve engineering problems, evaluate a wide range of potential solutions for those problems and arrive at feasible, optimal solutions after considering public health and safety, cultural, societal and environmental factors in the core areas of expertise.

PO4 Research Skill

Extract information pertinent to unfamiliar problems through literature survey and experiments, apply appropriate research methodologies, techniques and tools, design, conduct experiments, analyse and interpret data, demonstrate higher order skill and view things in a broader perspective, contribute individually/in group(s) to the development of scientific/technological knowledge in one or more domains of engineering.

PO5 Usage of modern tools

Create, select, learn and apply appropriate techniques, resources, and modern engineering and IT tools, including prediction and modeling, to complex engineering activities with an understanding of the limitations.

PO6 Collaborative and Multidisciplinary work

Possess knowledge and understanding of group dynamics, recognise opportunities and contribute positively to collaborative-multidisciplinary scientific research, demonstrate a capacity for self-management and teamwork, decision-making based on open-mindedness, objectivity and rational analysis in order to achieve common goals and further the learning of themselves as well as others.

PO7 Project Management and Finance

Demonstrate knowledge and understanding of engineering and management principles and apply the same to one's own work, as a member and leader in a team, manage projects efficiently in respective disciplines and multidisciplinary environments after consideration of economical and financial factors.

PO8 C**ommunication**

Communicate with the engineering community, and with society at large, regarding complex engineering activities confidently and effectively, such as, being able to comprehend and write effective reports and design documentation by adhering to appropriate standards, make effective presentations, and give and receive clear instructions.

PO9 Life-long Learning

Recognize the need for, and have the preparation and ability to engage in life-long learning independently, with a high level of enthusiasm and commitment to improve knowledge and competence continuously.

PO10 Ethical Practices and Social Responsibility

Acquire professional and intellectual integrity, professional code of conduct, ethics of research and scholarship, consideration of the impact of research outcomes on professional practices and an understanding of responsibility to contribute to the community for sustainable development of society.

PO11 Independent and Reflective Learning

Observe and examine critically the outcome s of one's actions and make corrective measures subsequently, and learn from mistakes without depending on external feedback.

M.E./M.Tech Programme Structure (CBCS)

Credit Distribution:

S.No	Category		Credits
A.	**Foundation Course**		**3 - 6**
B.	**Programme Core Courses***		**19 – 25**
C.	**Elective Courses**		**17 – 23**
	a.	Programme Elective	15 – 21
	b.	Open Elective	2 – 6
D.	**Common Core Course**		**2**
E.	**Mini Project and Dissertation**		**27**
E	Value Added Courses (Not to be included in CGPA) - Mandatory		**4**
	Minimum Credits to be earned for the award of the degree		**68** (from A to E) and 4 (from F)

*TCP and Laboratory courses are Mandatory in the Programme Core Courses.

Credit Details:

Theory: 3 Credits

Theory Cum Practical (TCP) : 3 Credits,

Lab: 2 Credits

Open Elective: 2 Credits

Mini Project: 2 Credits

Dissertation Phase I: 10 Credits

Dissertation Phase I: 15 Credits

Common Core: Research Methodology and IPR: 2 Credits

Scheduling of Courses

Semester	Theory					Theory Cum Practical	Laboratory	Project
I (17)	18IS110 Probability, Statistics and Graph Theory (3 Credits)	18IS120 Distributed and Cloud Computing (3 Credits)	18IS130 Cryptography and Network Security (3 Credits)	18ISPX0 Prog. Elective 1 (3 Credits)	-	18IS160 Algorithm Design Techniques (3 Credits)	18IS170 Cryptography and Network Security Lab (2 Credits)	-
II (21)	18IS210 Cyber Forensics (3 Credits)	18ISPX0 Prog. Elective 2 (3 Credits)	18ISPX0 Prog. Elective 3 (3 Credits)	18ISPX0 Prog. Elective 4 (3 Credits)	18PG250 Common Core (2 Credits)	18IS260 Data Analytics (3 Credits)	18IS270 Ethical Hacking and Cyber Forensics Lab (2 Credits)	18IS280 Mini Project (2 Credits)
III (15)	18ISPX0 Prog. Elective 5 (3 Credits)	-	-	-	18PGPX0 Open Elective (2 Credits)	-	-	18IS380 Dissertation Phase I (10 Credits)
IV (15)	-	-	-	-	-	-	-	18IS480 Dissertation Phase II (15 Credits)

List of Electives

Programme Elective 1:

- Security with Internet of Things
- Mobile and Wireless Security
- Secure Software Engineering
- Advanced Cryptography
- Biometrics
- Cloud Security
- Cyber Physical Systems
- Database Security and Access control
- Identity and Access Management
- Malware Analysis
- Security Assessment and Risk Analysis
- Secure Coding Practices
- Secure Network Management
- Steganography and Digital watermarking
- System Security

Programme Elective 2:

- Artificial Intelligence
- Augmented Reality
- Cognitive Science
- Data Sciences
- Deep Learning
- Enterprise Computing
- Information Theory and Coding
- Machine Learning
- Software Defined Networks
- Soft Computing

18IS110	Probability, Statistics and Graph Theory	Category	L	T	P	Credit
		FC	3	0	0	3

Preamble

This course is intended to provide the foundation on topics in applied probability and various statistical methods which form the basis for many other areas in the mathematical sciences including statistics and graph theory. As application of machine learning case studies in Bioinformatics will be analyzed.

Prerequisite

Discrete Mathematics, Basic Probability theory.

Course Outcomes

On successful completion of the course, students will be able to

Course Outcomes		Bloom's Level	Expected Proficiency	Expected Level of Attainment (in %)
CO1	Compute transition probabilities and limiting probabilities of various process.	Apply	B	90
CO2	Find the sampling distributions of estimators and to estimate the moments	Apply	B	90
CO3	identify the methods of statistical inference, to apply principal component analysis and to solve over fitting model. .	Apply	B	95
CO4	Aapply the knowledge of Graph Theory in to model a real time problem..	Apply	B	85
CO5	Use machine learning techniques to analyse genome structure.	Apply	B	95

apping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	S	M	L						L		
CO2	S	L	L						M		
CO3	S	M	L						L		
CO4	S	M	L						M		
CO5	S	M	L						M		

S - Strong, M – Medium, L – Low

Assessment Pattern

Bloom's Assessment Category	CAT 1	CAT 2	CAT 3	Terminal Exam
Remember	10	10	0	0
Understand	30	30	30	30
Apply	60	60	70	70
Analyze	0	0	0	0
Evaluate	0	0	0	0
Create	0	0	0	0

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Define transition probability matrix.
2. Describe the Chapman–Kolmogorov equation with its applications.
3. Given a two state Markov chain with the transition probability matrix $P = \begin{bmatrix} 1-a & a \\ b & 1-b \end{bmatrix}$, $0 \le a,\ b \le 1,\ |1-a-b| < 1$ the n-step transition probability matrix Find P(n).
4. Define X_n as the state of the system after the n^{th} state change, so that $X_n = \begin{Bmatrix} 0, \text{ if system is running} \\ 1, \text{ if system is under repair} \\ 2, \text{ if system is idle} \end{Bmatrix}$. Assume that the matrix P is $P = \begin{bmatrix} 0 & \frac{1}{2} & \frac{1}{2} \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$. Draw the state diagram and compute the matrix P^n.

Course Outcome 2 (CO2):

5. Given that the population X has the Cauchy distribution, show that the sample mean X has the same distribution.
6. Show that the method-of-moments estimators of the population mean and of the population variance are given by the sample mean, X and $(n-1)S^2/n$, respectively. Show that the method-of-moments estimator of the population variance is biased.
7. Show that the maximum-likelihood estimator of the mean life θ with a replacement test until r failures is $\Theta = \frac{nT_r}{r}$, where the random variable T_r denotes the time for the r^{th} failure from the beginning of the experiment.
8. Explain the terms Efficiency and Consistency of the system.

Course Outcome 3 (CO3):

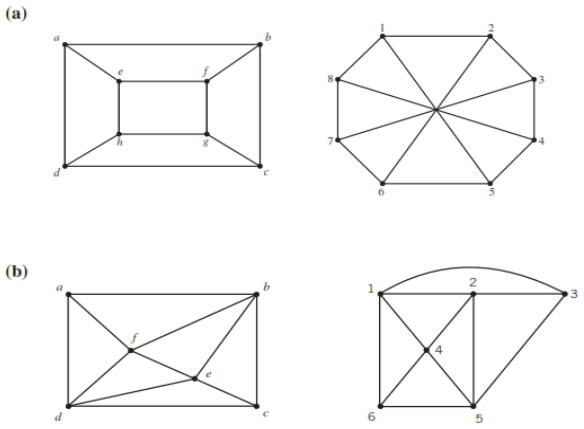
9. What is over fitting and how does it occur?
10. Describe when a model be identified as over fitted.
11. Explain at what point in the Principal Component Analysis process can we decide to
12. Compress the data? Demonstrate the PCA effect of
13. Compute the regression equation and coefficients for the following data from **n** = 5 hospitals in India are used to assess factors related to the likelihood that a hospital patients acquires an infection while hospitalized. The variables here are **y** = infection risk, $\mathbf{x}_1$ = average length

of patient stay, $\mathbf{x}_2$ = average patient age, $\mathbf{x}_3$ = measure of how many x-rays are given in the hospital

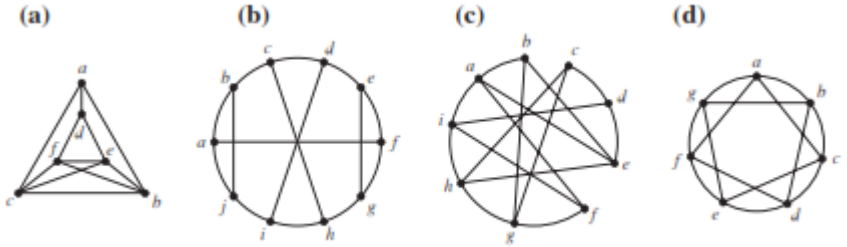
ID	STAY	AGE	InfctRsk	Xray
1	7.13	55.7	4.1	279
2	8.82	58.2	1.6	80
3	8.34	56.9	2.7	107
4	8.95	53.7	5.6	147
5	11.2	56.5	5.7	180

Course Outcome 4(CO4):

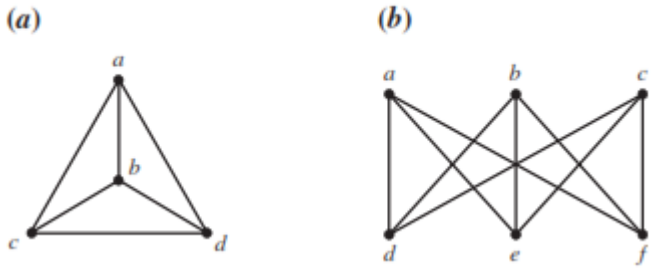
14. Which of the following graphs are isomorphic?
15.



16. Which of the following graphs are planar? Find $K_{3,3}$ or K_5 configurations in the nonplanar graphs.(almost all are $K_{3,3}$)



17. Find a minimal edge coloring of the following graphs (color edges so that edges with a common end vertex receive different colors).

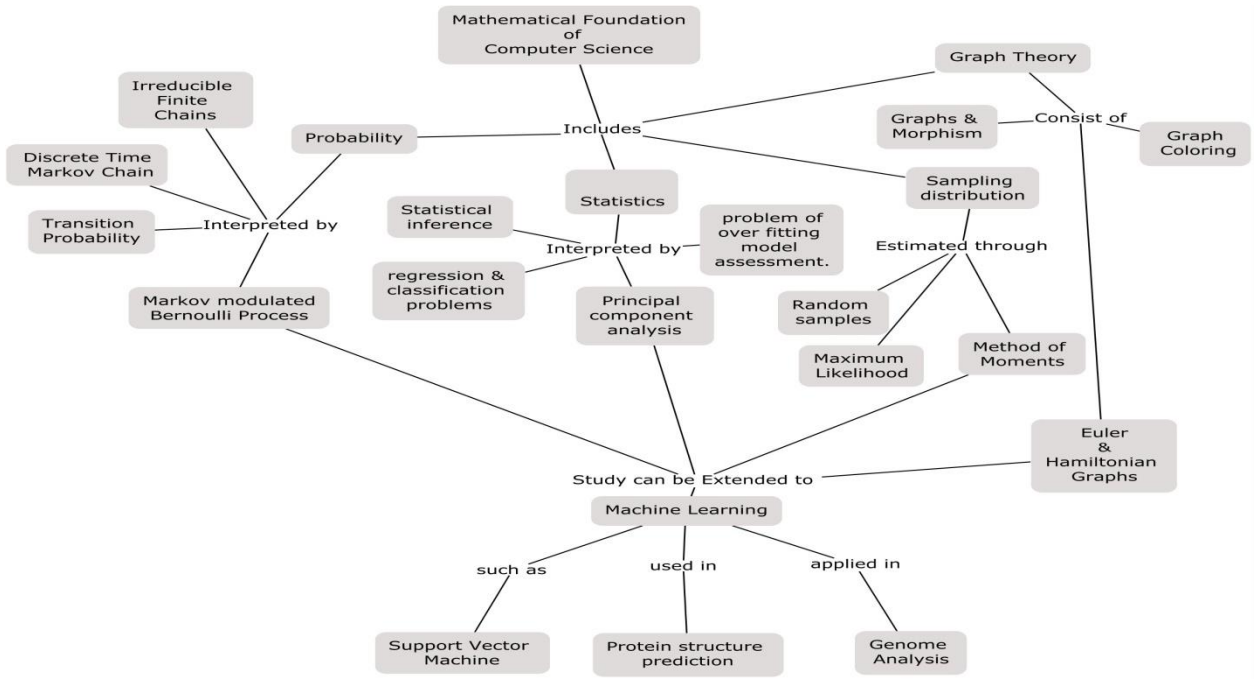
18. 

19.
20. How many different Hamilton circuits are there in K_n, a complete graph on n vertices?
21.

Course Outcome 4 (CO4):

22. Write any two techniques in Machine Learning.
23. Discuss the statistical inference in protein structure of the given DNA sequence?
24. Explain the applications of Hidden Markov Model in Gene sequence.
25. Describe the heuristic methods of sequence alignment? How does the genome analyzed by means of computational tools?

Concept Map



Syllabus

Probability:– Discrete time Markov Chain - Computation of n-step Transition Probabilities - State Classification and Limiting Probabilities - Distribution of Times between State Changes - Markov Modulated Bernoulli Process - Irreducible Finite Chains with Aperiodic States

Sampling distribution -Random samples, sampling distributions of estimators, Methods of Moments and Maximum Likelihood,

Statistics: Statistical inference , Introduction to multivariate statistical models: regression and classification problems, principal components analysis, The problem of over fitting model assessment.

Graph Theory: Isomorphism – Planar graphs- Graph colouring- Hamilton circuits and Euler cycles- Permutations and Combinations with and without repetition-

Machine Learning in Bioinformatics: Support Vector Machine- Prediction of Protein Secondary Structure of DNA sequence - Genome analysis with software tools-Case Study

Text Books

1. K. Trivedi. Probability and Statistics with Reliability, Queuing, and Computer Science Applications. John Wiley & Sons 2016.
2. Alan Tucker, Applied Combinatorics, 6th Edition John Wiley & Sons 2012.
3. Pierri Baldi and SorenBrunak , Bioinformatics-Machine Learning Approach 2nd Edition (E-book).

References

1. John Vince, Foundation Mathematics for Computer Science, Springer.
2. Devore, J. L.,- Probability and Statistics for Engineering and the Sciences, 8th Edition, Cengage Learning, 2014.
3. Gupta S.C. and Kapoor V.K., Fundamentals of Mathematical Statistics, Sultan and Sons, New Delhi, 2001.

Course Contents and Lecture Schedule

Module No	Topic	No. of Lecture Hours
1	Probability	
1.1	Discrete time Markov Chain	1
1.2	Computation of n-step Transition Probabilities	2
1.3	State Classification and Limiting Probabilities	2
1.4	Distribution of Times Between State Changes	1
1.5	Markov Modulated Bernoulli Process	2
1.6	Irreducible Finite Chains with Aperiodic States	1
2	Sampling distribution	
2.1	Random samples	1
2.2	Sampling distributions of estimators	2
2.3	Method of moments	2
2.4	Maximum Likelihood	2
3	Statistics	
3.1	Statistical inference	1
3.2	Introduction to multivariate statistical models	1
3.3	Regression and classification problems	2

3.4	Principal components analysis	2
3.5	The problem of over fitting model assessment	1
4	Graph Theory	
4.1	Isomorphism	1
4.2	Planar graphs	1
4.3	Graph coloring	1
4.4	Hamilton circuits and Euler cycles	2
4.5	Permutations and Combinations with and without repetition	2
5	Machine Learning in Bioinformatics	
5.1	Support Vector Machine	2
5.2	Prediction of Protein Secondary Structure of DNA sequence	1
5.3	Genome analysis with software tools	1
5.4	Case study	2
	Total	36

Course Desginers

1. S.Jeya Bharathi sjbmat@tce.edu
2. M.Kameswari mkmat@tce.edu
3. A.P.Pushpalatha appmat@tce.edu

18IS120	DISTRIBUTED AND CLOUD COMPUTING	Category	L	T	P	Credit
		PC	3	0	0	3

Preamble

The course aims to provide an understanding of the principles of distributed systems and cloud computing architecture, algorithms and ways of meeting the demands of contemporary distributed applications in the perspective of scalability, heterogeneity, failure and recovery. This course also covers issues and solutions related to the design and the implementation of distributed applications using parallel programming models and apply them into modern deployment tools

Prerequisite

NIL

Course Outcomes

On successful completion of the course, students will be able to

Course Outcomes		Bloom's Level	Expected Proficiency	Expected Level of Attainment (in %)
CO1	Explain the characteristics and models of distributed systems	Understand	A	90
CO2	Choose an appropriate service model to deploy an application in cloud environment.	Apply	A	80
CO3	Analyze the different algorithms and techniques for the design and development of distributed systems subject to specific design and performance constraints.	Analyze	B	70
CO4	Develop parallel programs using OpenMP and MPI constructs (CO4)	Apply	B	70
CO5	Write a parallel program for the given sequential task using GPU programming model	Apply	B	70
CO6	Develop and deploy an application in modern distributed platform with appropriate tools. (CO6)	Apply	A	80

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	M										
CO2	S	S	S	M	S	M			M		M
CO3	S	S	S	S	M	L			M		M
CO4	S	S	M	M	L				M		M
CO5	S	S	M	M	M				M		L
CO6	S	S	S	S	S	S	L	S	S	M	M

S - Strong, M – Medium, L – Low

Assessment Pattern

Bloom's Assessment Category	CAT 1	CAT 2	CAT 3	Terminal Exam
Remember	**20**	**20**	**20**	**20**
Understand	**30**	**20**	**20**	**20**
Apply	**50**	**40**	**40**	**40**
Analyze	**-**	**20**	**20**	**20**
Evaluate	**-**	**-**	**-**	**-**
Create	**-**	**-**	**-**	**-**

Course Level Assessment Question CO6 is assessed through Mini-project.

Mini-project Details

1. Team formation (Two per Team)
2. Problem Identification, Related work from IEEE and Science Direct
3. Identify the various components for the selected application with all distributed concepts
4. Deploy in the cloud environment.

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. List out the challenges in designing distributed systems.
2. An alternative definition for a distributed system is that of a collection of independent computers providing the view of being a *single system,* that is, it is completely hidden from users that there even multiple computers. Give an example where this view would come in very handy.
3. Define Cloud computing and explain essential characteristics of cloud computing.
4. Compare and contrast client-server, cluster, grids.

Course Outcome 2 (CO2):

5. Propose several ways of measuring cloud service performance and the importance of service level agreements
6. Contrast the different categories of cloud computing services
7. Prepare the report for Resource Provisioning and Platform Deployment for any Cloud Application.
8. Develop a program to count the frequency of a word in a dictionary using MapReduce framework.

Course Outcome 3(CO3):

9. Show that in Lamport‟s algorithm if a site Si is executing the critical section, then Si‟s request need not be at the top of the request_queue at another site Sj . Is this still true when there are no messages in transit?
10. Why is it difficult to keep a synchronized system of physical clocks in distributed systems?
11. Consider the behavior of two machines in a distributed system. Both have clocks that are supposed to tick 1000 times per millisecond. One of them actually does, but the other ticks only 990 times per millisecond. If UTC updates come in once a minute, what is the maximum clock skew that will occur?
12. Identify the requirements of mutual exclusion algorithm.

Course Outcome 4 (CO4):

13. Identify OpenMP directives for parallelization and write a program in C to illustrate the usage of work sharing constructs.
14. Write a simple program to illustrate the Blocking and Non-Blocking message passing directives.
15. Develop a Matrix multiplication program using MPI Libraries.

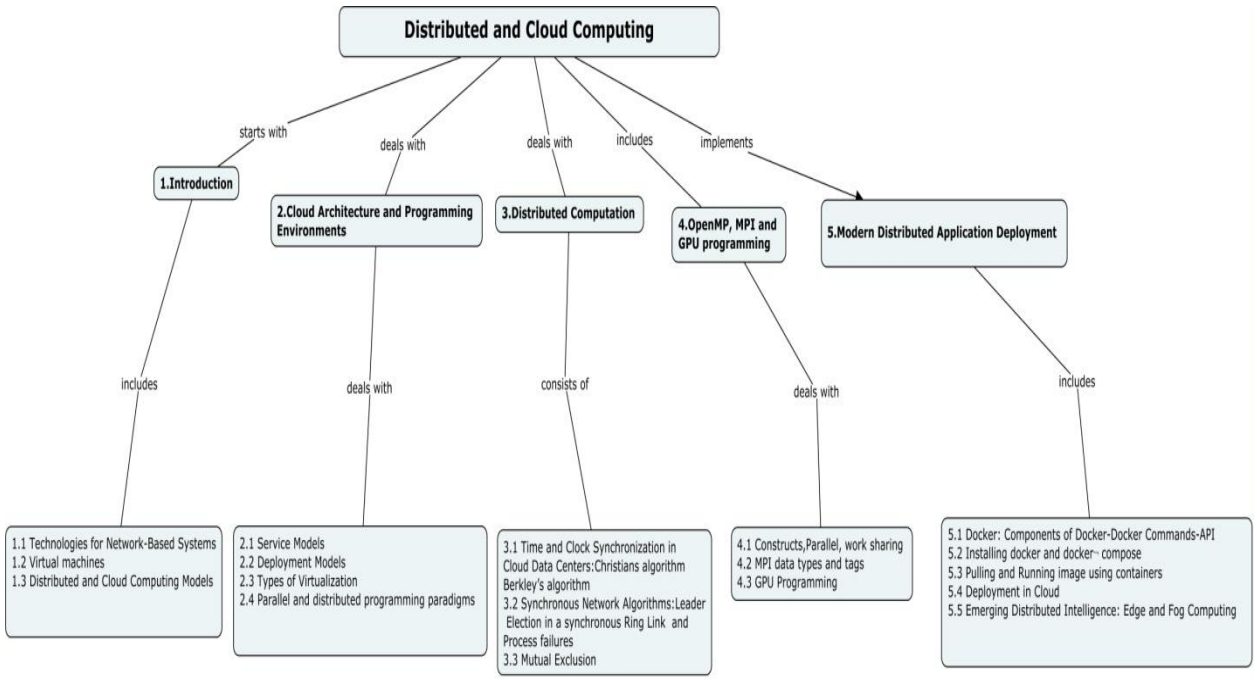
Course Outcome 5 (CO5):

16. Write a program that will get an input N and generate a randomized vector V of length N. It should then compute the maximum value in V on the CPU and on the GPU. The program should output the two computed maximum values as well as the time taken to find each value (Apply)
17. Summarize the CUDA programming model with a sample program and determine its efficiency.
18. Develop the sliding window sum problem with CUDA with its efficieny.
19. Compare and contrast GPU versus CPU in terms of speed, computation and memory.

Course Outcome 6 (CO6):

20. Build a Distributed application and deploy in the suitable platform
21. Make use of Docker how we can deploy the application and list out the essential features.
22. Apply the edge computing concept of device control in mobile distributed environment.
23. Create a simple application that includes the computation, storage and networking services between end devices using fog computing.

Concept Map



Syllabus

Introduction to Distributed Systems and Cloud Computing: Technologies for Network-Based Systems: multi-core and multi-threading; virtual machines-Distributed and Cloud Computing Models: client-server; clusters; grids; peer-to-peer - Examples of distributed systems

Cloud Architecture and Programming Environments: Service Models: IaaS; PaaS; SaaS Deployment Models: public clouds; private clouds; hybrid clouds - Virtualization: Level of virtualization; virtualization support at the OS level, middleware support; virtualization of CPU, memory, and I/O devices; virtualization tools, Parallel and distributed programming paradigms: Map Reduce, Hadoop.

Distributed Computation: Time and Clock Synchronization in Cloud Data Centers: Synchronization in the cloud, Key challenges, External and Internal clock synchronization, Christians algorithm, Berkley's algorithm, Datacenter time protocol (DTP), Logical ordering, Lamport timestamps, Vector timestamps Synchronous Network Algorithms: Synchronous Network Model, Leader Election in a synchronous Ring, Link and Process failures. Distributed Mutual Exclusion: Mutual Exclusion in Cloud, Central algorithm, Ring-based Mutual Exclusion, Lamport's algorithm, Ricart-Agrawala's algorithm.

OpenMP, MPI and GPU programming: Constructs –Parallel, work sharing and Synchronization constructs. MPI data types and tags, environment management routines. GPU: GPU architecture; Introduction to CUDA programming; Concept of SIMD and SIMT computation; Thread blocks.

Modern Distributed Application Deployment: Docker: Components of Docker-Docker Commands-API-Installing docker and docker compose - Pulling and Running image using containers- Deployment in Cloud - Emerging Distributed Intelligence**:** Edge and Fog Computing

Text Books

1. Kai Hwang, Geoffrey.C.Fox and Jack J.Dogarra, "Distributed and Cloud Computing From Parallel Processing to the Internet of Things", Morgan Kaufmann Publishers, Elsevier,2013.
2. Thomas Erl and Ricardo Puttini ,"Cloud Computing: Concepts, Technology and Architecture" URC Press,2014**.**
3. Ajay D. Kshemkalyani and Mukesh Singhal , "Distributed Computing Principles, Algorithms, and Systems", Cambridge University Press, Fifth Edition,2011.

References

1. Sukumar Ghosh, "Distributed Systems: An Algorithmic approach", 2006 CRC Press.
2. M.L.Liu, "Distributed Computing Principles and Applications", Pearson Education, 2004.
3. .http://www.cdk5.net/wp/instructorsguide/presentationpoints/pointspresetationpoints-chapter-2
4. http://www.slideshare.net/zbigniew.jerzak/clock-synchronization-in-distributedsystems
5. http://www.slideshare.net/sriprasanna/clock-synchronization-distributed-computing
6. Cloud computing and Distributed systems: http://nptel.ac.in/courses/106106107/
7. https://medium.com/google-cloud/modern-distributed-application-deployment-with-kubernetes-and-mongodb-atlas-4ec9eff5bab

Course Contents and Lecture Schedule

Module No	Topic	No. of Lecture Hours
1	**Introduction to Distributed Systems and Cloud Computing (4)**	
1.1	Technologies for Network-Based Systems: multi-core and multi-threading	1
1.2	Virtual machines	1
1.3	Distributed and Cloud Computing Models: client-server; clusters; grids; peer-to-peer, Examples of distributed systems	2
2	**Cloud Architecture and Programming Environments**	
2.1	Service Models: IaaS; PaaS; SaaS	2
2.2	Deployment models in Cloud: public clouds; private clouds; hybrid clouds	2
2.3	Types of Virtualization	2
2.4	Parallel and distributed programming paradigms: Map Reduce, Hadoop.	2
3	**Distributed Computation (9)**	
3.1	Time and Clock Synchronization in Cloud Data Centers: Synchronization in the cloud, Key challenges, External and Internal clock synchronization	1
3.2	Christians algorithm, Berkley's algorithm	1
3.3	Datacenter time protocol, Logical ordering, Lamport timestamps, Vector timestamps	1
3.4	Synchronous Network Algorithms: Synchronous Network Model, Leader Election in a synchronous Ring	1
3.5	Link and Process failures	1
3.6	Mutual Exclusion: Mutual Exclusion in Cloud, Central algorithm	1
3.7	Ring-based Mutual Exclusion	1
3.8	Lamport's algorithm, Ricart-Agrawala's algorithm	1
4	**OpenMP, MPI and GPU programming (7)**	
4.1	Constructs –Parallel, work sharing and Synchronization constructs	2
4.2	MPI data types and tags, environment management routines.	2
4.3	GPU: GPU architecture; Introduction to CUDA programming	2
4.4	Concept of SIMD and SIMT computation; Thread blocks	1
5.	**Modern Distributed Application Deployment (8)**	
5.1	Docker: Components of Docker-Docker Commands-API	1
5.2	Installing docker and docker compose	2
5.3	Pulling and Running image using containers	2
5.4	Deployment in Cloud	1
5.5	Emerging Distributed Intelligence**:** Edge and Fog Computing	2
	Total Hours	36

Course Designers

1. S.Padmavathi spmcse@tce.edu
2. K.Indira kiit@tce.edu

18IS130	CRYPTOGRAPHY AND NETWORK SECURITY	Category	L	T	P	Credit
		PC	3	0	0	3

Preamble

The course on Cryptography and Network Security aims at exploring the various cryptographic algorithms deployed in offering confidentiality, integrity, authentication and nonrepudiation. The mathematical essentials required for understanding of cryptographic algorithms is covered in detail. The course will enable the students to understand, develop and deploy countermeasures to mitigate the risks inherent in the transmission, storage and retrieval of sensitive information and will provide the foundation for doing research in Information security.

Preamble

Nil

Course Outcomes

On successful completion of the course, students will be able to

Course Outcomes		Bloom's Level	Expected Proficiency	Expected Level of Attainment (in %)
CO1	Appreciate the usage of Number theory in design of cryptographic algorithms.	Apply	B	70
CO2	Deploy measures for data protection by ensuring t confidentiality, integrity, authentication and non-repudiation.	Apply	B	70
CO3	Examine the strength of any cryptographic algorithm by crypt analysis.	Analyze	B	70
CO4	Use various authentication and security protocols such as SSL, IP Sec etc., at different layers of TCP/IP stack to develop security solutions.	Apply	B	70
CO5	Comprehend the usage of firewalls and Intrusion Detection Systems for securing data	Understand	B	75
CO6	Write a security analysis report on security attacks and vulnerabilities of any information system and provide suitable solutions.	Analyze	B	70

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	S	M	M		L						
CO2	S	M	M		L						
CO3	S	S	M	M	S						
CO4	S	M	L								
CO5	M										
CO6	S	S	S	M	S	M		M	M	M	

S - Strong, M – Medium, L – Low

Assessment Pattern

Bloom's Assessment Category	CAT 1	CAT 2	CAT 3	Terminal Exam
Remember	20	20	10	10
Understand	20	20	20	20
Apply	40	40	40	40
Analyze	20	20	30	30
Evaluate	0	0	0	0
Create	0	0	0	0

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Consider the field GF(2^4). Let field multiplication be performed modulo the irreducible polynomial $x^4 + x + 1$. Compute each of the following.
    - (1100) + (1001)
    - (1011) * (0111)
    - $(1101)^{-1}$
2. Compute the result of the following:
    - 145^{204} mod 101 using Fermat's theorem.
    - 44^{-1} mod 667 using Euler's theorem.
    - The count of relative primes to 10000.
    - Any two primitive roots of Z_{19}.
3. Compute the following:
    - GCD of $x^4 + x^3$ with respect to the modulus $x^8 + x^4 + x^3 + x^2 + 1$.
    - Product of the two polynomials $(4x^7 + 4x^2 + 3)$ and $(3x^3 + 9)$ with coefficients in Z_5.

Course Outcome 2 (CO2):

4. Consider the elliptic curve defined by the equation $y^2 = x^3 + 9x + 17$ with a modulus of p=23 and G=(16,5).

- Prove mathematically that the session keys generated at both the sender and receiver sides are exactly the same.
- Determine any four affine points on the curve.
- If the private key of User A is 2, What is his public key?

5. Evaluate the output of one round of Advanced Encryption Standard for the given plain text and round key:

PLAIN TEXT			
01	63	F1	96
55	24	3A	62
F4	8A	DE	4D
CC	BA	88	03

ROUND KEY			
EE	EA	2F	D8
61	FE	62	E3
AC	1F	A6	9D
DE	4B	E6	92

6. Compute the hash value of the message M=CRYPTOGRAPHY… using Secure Hash Algorithm (SHA) for one step. Draw the schematic diagram, Compute the relevant parameters, assume initial Values of buffers and the function as (B && C)|| (B && D)|| (C && D).

Course Outcome 3 (CO3):

7. Consider a crypto system in which the encryption formula is C=KP mod m where C,K,P,m are integers. Identify the decryption formula and analyze the possible number of keys if the modulus is m=19.
8. Is it possible to design a protocol that accomplishes both authentication and session key exchange with only two messages and without timestamps? Consider each of the following two cases separately.
    - The two parties share a long term secret.
    - Both communicating parties have a public key – private key pair. Each party knows other's public key.
9. Assume that passwords are limited to the use of 95 printable ASCII characters and that all the passwords are 10 characters in length. Assume a password cracker with an encryption rate of 6.4 million encryptions per second. How long will it take to test exhaustively all possible passwords on a UNIX system?

Course Outcome 4 (CO4):

10. The sending of an email from Alice to Bob is a store and retrieve activity wherein Alice can send a mail at one instant of time and Bob can check his mail at any other instant of time. Since a session could not be established between Alice and Bob, identify a suitable cryptographic protocol to handle this situation and detail the steps involved.

11. In developing a website of an online retail store, elaborate on the procedure you would adopt for securing online payments made by your customers.
12. Company policy requires two hosts, A and B in two different branches of an organization to communicate securely over the Internet using IPSec. Which of the four options would be most appropriate – AH in tunnel mode, AH in transport mode, ESP in transport mode or ESP in tunnel mode? Explain your choice. Show all the headers that are inserted in communication and the scope of integrity checking and encryption.

Course Outcome 5 (CO5):

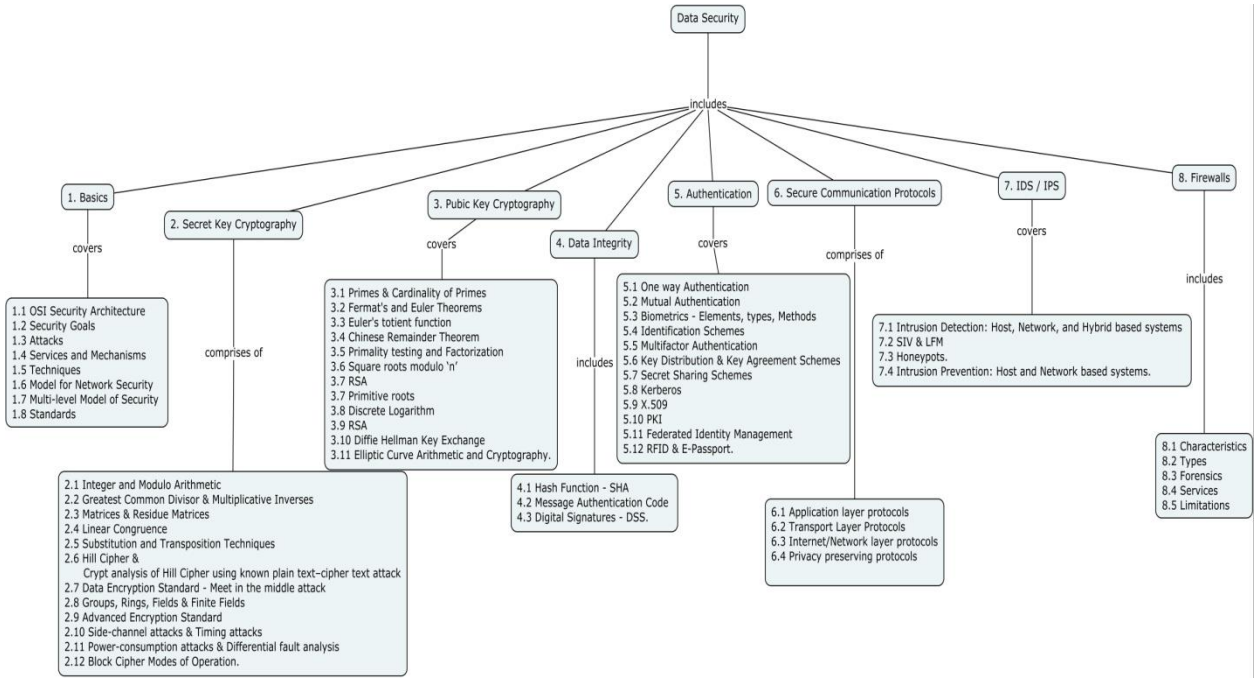
13. Develop rules for the following cases in a packet filtering firewall:
    a. Allow inbound mails excepting a particular external host SPIGOT.
    b. Any inside host can send mail to outside
    c. Allow IP packets where the source IP address is one of a list of designated Internal hosts and the destination TCP port number is 25.
    d. In handling ftp connections, allow
        i. Packets that originate internally.
        ii. Reply packets to a connection initiated by an internal machine.
        iii. Packets destined for a high numbered port on an internal machine.
14. Compare the packet marking versus packet logging schemes for IP trace back in respect to the probability of success, cost, ease of deployment and performance overheads.
15. Compare and contrast statistical anomaly detection vs. rule based anomaly detection.

Course Outcome 6 (CO6):

16. Consider a scenario with multiple users and multiple servers in an organization such as a University campus. A user, once logged in, may then wish to access different resources such as an e-mail server or a file server in the course of that login session. Suggest a suitable authentication protocol and elaborate its working to handle the above situation.
17. When a customer shops online, the following security services are desired:
    a. The customer needs to be sure that the server belongs to the actual vendor and not an impostor.(Entity Authentication)
    b. The customer and the vendor need to be sure that the contents of the message are not modified during transmission. (Message Integrity)
    c. The customer and the vendor needs to be sure that an impostor does not receive sensitive information such as credit card number (Confidentiality)

    Suggest and deploy a suitable protocol to offer the above end to end security requirements
18. Prepare a security analysis report on the threats and vulnerabilities involved in an online voting system.

Concept Map



Syllabus

BASICS OF INFORMATION SECURITY – OSI Security Architecture - Security Goals - Attacks - Services and Mechanisms - Techniques - Model for Network Security - Multi-level Model of Security - Standards.

SECRET KEY CRYPTOGRAPHY - Mathematics for Cryptography - Integer and Modulo Arithmetic - Greatest Common Divisor - Multiplicative Inverses - Matrices - Residue Matrices - Linear Congruence - Substitution and Transposition Techniques - Hill Cipher - Crypt analysis of Hill Cipher using known plain text–cipher text attack - Data Encryption Standard - Meet in the middle attack - Groups, Rings, Fields - Finite Fields - Advanced Encryption Standard - - Side-channel attacks - Timing attacks - Power-consumption attacks - Differential fault analysis - Block Cipher Modes of Operation.

PUBLIC KEY CRYPTOGRAPHY - Primes - Cardinality of Primes - Fermat's and Euler Theorems - Euler's totient function - Chinese Remainder Theorem - Primality testing and Factorization - Square roots modulo 'n' - Primitive roots - Discrete Logarithm - RSA - Elliptic Curve Arithmetic and Cryptography.

DATA INTEGRITY – Hash Function - SHA - Message Authentication Code - Digital Signatures - DSS.

AUTHENTICATION – One way Authentication - Mutual Authentication - Biometrics - Elements, types, Methods - Identification Schemes - Multifactor Authentication - Key Distribution - Key Agreement Schemes - Secret Sharing Schemes - Kerberos - X.509 - PKI - Federated Identity Management - RFID - E-Passport.

SECURE COMMUNICATION PROTOCOLS - Application layer protocols: E-mail security: PGP ,HTTPS , SSH, Transport layer Protocols - SSL/TLS. Attacks on TLS: Downgrade attacks - Certificate forgery - Implications of stolen root certificates - Certificate transparency. Internet/Network layer: IPsec - VPN. Privacy preserving protocols: Mixnet - Tor - Off-the-record message - Signal.

INTRUSION DETECTION AND PREVENTION – Intrusion Detection: Host, Network, and Hybrid based systems - SIV - LFM - Honeypots. Intrusion Prevention: Host and Network based systems.

FIREWALLS - Characteristics - Types - Forensics - Services - Limitations

Text Books

1. Behrouz. A. Foruzan and Debdeep Mukhopadhyay, “Cryptography and Network Security”, Tata McGraw Hill , Third Edition, 2016.
2. Bernard L Menezes, and Ravinder Kumar “Cryptography, Network Security and Cyber Laws”, Cengage Learning India Pvt Limited, 2018.

References

1. William Stallings, “Cryptography and Network Security: Principles and Practice”, Prentice Hall,Seventh Edition, 2017.
2. Charlie Kaufman and Radia Perlman, Mike Speciner, “Network Security, Private Communication in Public World”, Prentice Hall India , Second Editon ,2002.
3. William Stallings, "Network Security Essentials: Applications and Standards", Prentice Hall, Sixth Edition, 2016.
4. Man Young Rhee, " Internet Security Cryptographic Principles, Algorithms and Protocols", Wiley, First Edition, 2003.
5. Douglas R. Stinson, “Cryptography Theory and Practice”, Third Edition, Chapman & Hall/CRC, 2006.
6. http://cse.iitkgp.ac.in/~debdeep/courses_iitkgp/Crypto/index.htm
7. http://nptel.ac.in/courses/106105031/
8. https://canvas.uw.edu/courses/1064488

Course Contents and Lecture Schedule

Module No.	Topic	No. of Lectures
1	**BASICS OF INFORMATION SECURITY**	
1.1 1.2 1.3 1.4	OSI Security Architecture Security Goals Attacks Services and Mechanisms	1
1.5 1.6	Techniques Model for Network Security	1
1.7 1.8	Multi-level Model of Security Standards.	

Module No.	Topic	No. of Lectures
2	**SECRET KEY CRYPTOGRAPHY**	
2.1 2.2	Mathematics for Cryptography Integer and Modulo Arithmetic Greatest Common Divisor and Multiplicative Inverses	1
2.3 2.4	Matrices - Residue Matrices Linear Congruence	1
2.5 2.6	Substitution and Transposition Techniques Hill Cipher	1
2.7	Crypt analysis of Hill Cipher using known plain text–cipher text attack	1
2.8	Data Encryption Standard	2
2.8	Meet in the middle attack	1
2.9	Groups, Rings, Fields - Finite Fields	1
2.10	Advanced Encryption Standard	1
2.11 2.12	Side-channel attacks - Timing attacks Power-consumption attacks - Differential fault analysis	1
2.13	Block Cipher Modes of Operation.	1
3	**PUBLIC KEY CRYPTOGRAPHY**	
3.1 3.2 3.3. 3.4	Primes - Cardinality of Primes Fermat's and Euler Theorems Euler's totient function Chinese Remainder Theorem	1
3.5 3.6	Primality testing and Factorization Square roots modulo ‘n’	1
3.7	RSA	1
3.8 3.9 3.10	Primitive roots Discrete Logarithm Diffie Hellman key Exchange	1
3.11	Elliptic Curve Arithmetic and Cryptography.	1
4	**DATA INTEGRITY**	
4.1 4.2	Hash Function - SHA Message Authentication Code	1
4.3	Digital Signatures - DSS.	1
5	**AUTHENTICATION**	
5.1 5.2	One way Authentication Mutual Authentication	1
5.3 5.4 5.5	Biometrics - Elements, types, Methods Multifactor Authentication Identification Schemes	1
5.6	Key Distribution and Key Agreement Schemes	1
5.7 5.8	Secret Sharing Schemes Kerberos	1
5.9	X.509	1
5.10	PKI	1
5.11	Federated Identity Management	1
5.12	RFID - E-Passport.	1
6	**SECURE COMMUNICATION PROTOCOLS**	
6.1	Application layer protocols: E-mail security: PGP	1

Module No.	Topic	No. of Lectures
6.1 6.1	HTTPS SSH	1
6.2	Transport layer Protocols - SSL/TLS	1
6.2	Attacks on TLS: Downgrade attacks - Certificate forgery - Implications of stolen root certificates - Certificate transparency.	1
6.3	Internet/Network layer: IPsec - VPN.	
6.4	Privacy preserving protocols: Mixnet - Tor - Off-the-record message - Signal	1
7 7.1	**INTRUSION DETECTION AND PREVENTION** Intrusion Detection: Host, Network, and Hybrid based systems	1
7.2 7.3	SIV - LFM Honeypots.	1
7.4	Intrusion Prevention: Host and Network based systems	
8 8.1 8.2 8.3 8.4 8.5	**FIREWALLS** Characteristics Types Forensics Services Limitations	1
Total Lecture Hours		36

Course Designers:

1. C.Jeyamala jeyamala@tce.edu
2. M.Thangavel mtit@tce.edu

18IS160	ALGORITHM DESIGN TECHNIQUES	Category	L	T	P	Credit
		PC	2	0	2	3

Preamble

The course on algorithm design techniques provides with an emphasis on algorithmic design in computing applications. This course covers five major algorithmic design techniques (ADT, skip list, text processing, graph algorithm, and network flows), with computability theory focusing on undecidability, computational complexity focusing on NP-completeness, and algorithmic techniques for intractable problems, including identification of structured special cases, approximation algorithms, and local search heuristics.

Prerequisite

Nil

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes for Theory		Bloom's Level	Expected Proficiency	Expected level of attainment (%)
CO1:	Practise appropriate data structures, understand the ADT/libraries, and use it to design algorithms for a specific problem.	Apply	B	75
CO2:	Experiment the necessary mathematical abstractions to solve problems using skip lists algorithms.	Apply	B	75
CO3:	Compute various text processing operations with algorithmic complexity and apply it for recent developments in the area of algorithmic design.	Apply	B	75
CO4:	Investigate the realm of using graph algorithms and network flow techniques by applying it for real time applications.	Apply	B	75

Course Outcomes for Practical		Bloom's Level	Expected Proficiency	Expected level of attainment (%)
CO5:	Examine different classes of problems concerning their computation difficulties.	Analyse	B	85
CO6:	Solve solutions for complex problems by utilizing appropriate algorithmic techniques with analysis of efficiency and proof of correctness.	Analyse	B	85

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	M	S	M		S						
CO2	M	S	M		S						
CO3	M	S	M		S						
CO4	M	S	M		S						
CO5	S	S	M		S			M	M	M	M
CO6	S	S	M		S			M	M	M	M

S- Strong; M-Medium; L-Low

Assessment Pattern

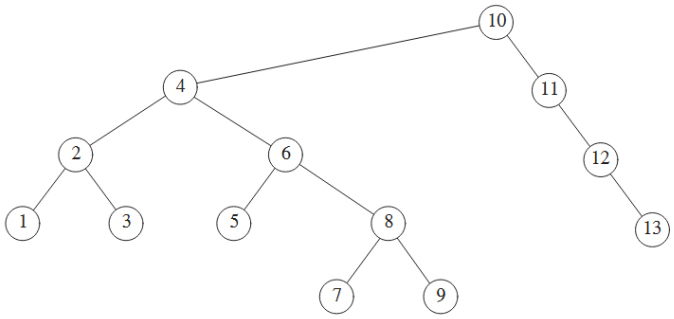
Bloom's Category	Continuous Assessment Tests			Practical Test	Terminal Examination
	1	2	3		
Remember	20	20	20	-	20
Understand	30	30	20	10	20
Apply	30	30	60	20	60
Analyse	0	0	0	70	0
Evaluate	0	0	0	0	0
Create	0	0	0	0	0

ATTAINMENT OF COURSE OUTCOME 5 AND 6 IS EVALUATED THROUGH MINI PROJECT WHICH INVOLVES DESIGN AND DEVELOPMENT OF ALGORITHMS FOR ANY REAL TIME APPLICATIONS.

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Demonstrate the result of accessing the keys 3, 9, 1, 5 in order in the splay tree in the below Figure and Show the result of deleting the element with key 6 in the resulting splay tree.

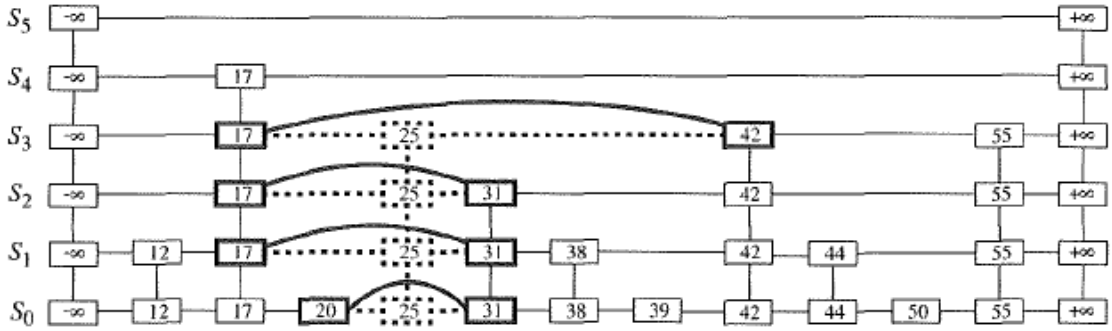


2. If a d-heap is stored as an array, for an entry located in position i, Identify the parents and children.
3. Compute the result of inserting 10, 12, 1, 14, 6, 5, 8, 15, 3, 9, 7, 4, 11, 13, and 2, one at a time, into an initially empty binary heap. Show the result of using the linear-time algorithm to build a binary heap using the same input.

4. Given input {4371, 1323, 6173, 4199, 4344, 9679, 1989} and a hash function h(x)=x(mod () 10), draw
    a. separate chaining hash table
    b. hash table using linear probing
    c. hash table using quadratic probing
    d. hash table with second hash function h2(x)=7−(xmod 7)

Course Outcome 2 (CO2):

5. Apply a suitable search method in a sorted linked list to search better than O(n) time.
6. Draw an example skip list resulting from performing the following sequence of operations on the skip list in Figure given below. removeEiement(38), i nsertltem(48,x), in sertltem(24,y), removeEiement(55). Assume the coin flips for the first insertion yield two heads followed by tails, and those for the second insertion yield three heads followed by tails.



7. Give a pseudo-code description of the removeElement dictionary operation, assuming the dictionary is implemented by a skip-list structure.
8. Give a pseudo-code description to count the number of equivalent elements in a deterministic skip list. Compare the performance of deterministic skip list with traditional searching mechanism.

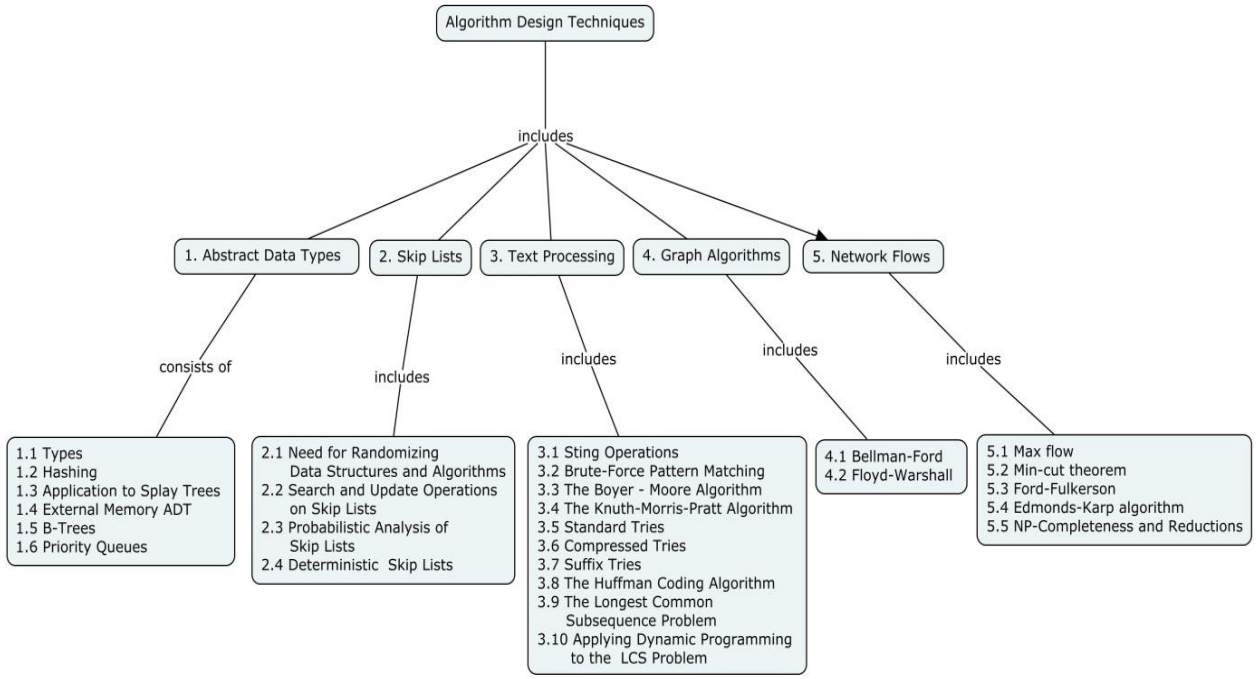
Course Outcome 3(CO3)

9. Describe an efficient algorithm to find the longest palindrome that is a suffix of a string T of length n. Recall that a palindrome is a string that is equal to its reversal. Identify the running time of the method.
10. Show that a sequence of n distinct numbers contains a decreasing or increasing subsequence of size at least $\lfloor\sqrt{n}\rfloor$.
11. Give a justification of why the KMP FailureFunction method runs in $O(m)$ time on a pattern of length m.
12. Modify the simplified Boyer Moore algorithm using ideas from the KMP algorithm so that it runs in $O\ (n\ +\ m)$ time.

Course Outcome 4(CO4)

13. Suppose that G=(V,E) is a tree, s is the root, and we add a vertex t and edges of infinite capacity from all leaves in G to t. Give a linear-time algorithm to find a maximum flow from s to t.
14. The baseball card collector problem is as follows: Given packets $P_1, P_2, \ldots . P_M$, each of which contains a subset of the year's baseball cards, and an integer, K ,is it possible to collect all the baseball cards by choosing $\leq K$ packets? Show that the baseball card collector problem is NP-complete.
15. The biconnected components of a graph, G, is a partition of the edges into sets such that the graph formed by each set of edges is biconnected. Modify the Bellman-ford algorithm to find the biconnected components instead of the articulation points.
16. A student needs to take a certain number of courses to graduate, and these courses have prerequisites that must be followed. Assume that all courses are offered every semester and that the student can take an unlimited number of courses. Given a list of courses and their prerequisites, compute a schedule that requires the minimum number of semesters.

Concept Map



Syllabus

Abstract Data Types - Types - Hashing -Application to Splay Trees - External Memory ADT - B-Trees - Priority Queues **Skip Lists** Need for Randomizing Data Structures and Algorithms - Search and Update Operations on Skip Lists - Probabilistic Analysis of Skip Lists - Deterministic Skip Lists –**Text Processing** Sting Operations - Brute-Force Pattern Matching - The Boyer - Moore Algorithm - The Knuth-Morris-Pratt Algorithm - Standard Tries - Compressed Tries - Suffix Tries - The Huffman Coding Algorithm - The Longest Common Subsequence Problem (LCS) - Applying Dynamic Programming to the LCS Problem. **Graph Algorithms** - Bellman-Ford - Floyd-Warshall.**Network Flows**- Max flow - min-cut theorem - Ford-Fulkerson - Edmonds-Karp algorithm - NP-Completeness and Reductions.

References

1. Mark Allen Weiss, Data Structures and Algorithm Analysis in C++, 4th Edition, Pearson, 2014
2. M T Goodrich, Roberto Tamassia, Algorithm Design and Applications, John Wiley New Edition, 2014.
3. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein, "Introduction to Algorithms", MIT Press, 3rd Edition, 2009.
4. Alfred V.Aho, John E. Hopcroft, 'The Design and Analysis of Computer Algorithms', Addison-Wesley Longman Publishing Co., 1st edition, 1974.
5. Jon Kleinberg, Eva Tardos, 'Algorithm Design', Pearson, 1st edition, 2006.
6. https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-851-advanced-data-structures-spring-2012/
7. https://www.coursera.org/learn/advanced-data-structures
8. https://www.coursera.org/specializations/data-structures-algorithms

Course Contents and Lecture Schedule

S.No	Topic	No.of Lectures
1.	**Abstract Data Types**	
1.1	Types	0.5
1.2	Hashing	1
1.3	Application to Splay Trees	1
1.4	External Memory ADT	1
1.5	B-Trees	1
1.6	Priority Queues	1
2.	**Skip Lists**	
2.1	Need for Randomizing Data Structures and Algorithms	0.5
2.2	Search and Update Operations on Skip Lists	1
2.3	Probabilistic Analysis of Skip Lists	1
2.4	Deterministic Skip Lists	1
3.	**Text Processing**:	
3.1	Sting Operations	0.5
3.2	Brute-Force Pattern Matching	1
3.3	The Boyer - Moore Algorithm	1
3.4	The Knuth-Morris-Pratt Algorithm	1
3.5	Standard Tries	1
3.6	Compressed Tries	1

S.No	Topic	No.of Lectures
3.7	Suffix Tries	1
3.8	The Huffman Coding Algorithm	1
3.9	The Longest Common Subsequence Problem (LCS)	1
3.10	Applying Dynamic Programming to the LCS Problem	0.5
4	**Graph Algorithms**	
4.1	Bellman-Ford	1
4.2	Floyd-Warshall	1
5	**Network Flows**	
5.1	Max flow, min-cut theorem	0.5
5.2	Ford-Fulkerson	1
5.3	Edmonds-Karp algorithm	1
5.4	Bipartite Matching	0.5
5.5	NP-Completeness and Reductions	1
Total		**24**

Lab Schedule

S. No	Name of Experiments	No.of hours
1.	Implement insertion, deletion, display and search operation in m-way B-tree (i.e. a non-leaf node can have at most m-children) for the given data (May be integer, float or String and Test the program for m = 3, 5, 7).	2
2.	Implement Binomial Heap / Max Heap / Fibonacci heap with its operations for the student structures database or for an employee management system.	2
3.	Demonstrate the operation of Splay tree (self-balancedBST).	1
4.	Demonstrate the working principle of skip listfor distributed systems, in which nodes of skip list represents the computer systems and the pointer represents network connection.	1
5.	Implement single-source shortest path in a weighted directed graph using Bellman-Ford algorithm	1
6.	Implement the working mechanism of Floyd-Warshall algorithm to find all-pairs shortest path.	1
7.	Implement all-pairs shortest path using dynamic-programming algorithm for matrix multiplication.	1
8.	Implement the working principle of Boyer-Moore algorithm to perform string matching.	1
9.	Solve NP complete for n Queens problem	1
10.	Implement Ford-Fulkerson algorithm to compute the maximum flow of a graph.	1
Total Sessions		**12**

Course Designers:

1. A.Sheik Abdullah asait@tce.edu
2. T.Manju tmanju@tce.edu
3. E.Ramanujam erit@tce.edu

18IS170	CRYPTOGRAPHY AND NETWORK SECURITY LAB	Category	L	T	P	Credit
		PC	0	0	4	2

Preamble

The laboratory course on Cryptography and Network security provides aims to provide hands on experience in communication security for computer systems and networks.. Practical exposure on usage of various network security services and tools for analysing security vulnerabilities and protection is also provided.

Prerequisite

Nil

Course Outcomes

On successful completion of the course, students will be able to

Course Outcomes		Bloom's Level	Expected Proficiency	Expected Level of Attainment (in %)
CO1	Make use of cryptography techniques to provide confidentiality for the given problem.	Apply	B	75
CO2	Practice hashing and digital signatures to provide authentication for the given scenario.	Apply	B	75
CO3	Inspect the strength of the cryptographic algorithm by cryptanalysis and OPENSSL	Analyze	B	75
CO4	Interpret the results of Network packet analyzer, and port scanner to identify the strength of the given network scenario.	Analyze	B	75
CO5	Configure Firewall, Intrusion Detection System and Log analysis tool to defend against security attacks.	Apply	B	75
CO6	Simulate the software vulnerabilities such as SQL injection, Cross site scripting using appropriate tool.	Apply	B	75
CO7	Examine the various security protocol validation tool and web server / application vulnerabilities.	Analyze	B	75

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	S	M	L		S			M	M	L	L
CO2	S	M	L		S			M	M	L	L
CO3	S	S	M		S			M	M	L	L
CO4	S	S	M		S			M	M	L	L
CO5	S	M	L		S			M	M	L	L
CO6	S	M	L		S			M	M	L	L
CO7	S	S	M		S			M	M	L	L

S - Strong, M – Medium, L – Low

List of Experiments

Exp No.	Topic	No. of Lab Hours
1	Implementation and Cryptanalysis of Hill Cipher to secure client-server communications	4
2	Implementation of Block cipher modes of operations using Data Encryption Standard (DES) and Advanced Encryption Standard (AES). (Use Standard crypto Libraries)	4
3	Implementation and Cryptanalysis of RSA cryptosystem for secure file transfer among 3 or more users.	4
4	Implementation of Diffie-Hellman Key exchange algorithm with Man in the Middle Attack	2
5	Apply Hashing techniques and Digital Signatures to design an secure communication by ensuring Message Authentication and Confidentiality. (Use Standard crypto Libraries)	4
6	Security Analysis of Cryptographic algorithms using OPEN SSL packages	4
7	Analysis of Secure Socket Layer and IPSec protocol using Network packet analyzer (Wireshark or equivalent tools)	4
8	Perform port scanning to identify live hosts and services	2
9	Simulation of SQL Injection attack using appropriate tool. (DVWA or equivalent tools)	2
10	Simulation of Cross-site scripting attack using appropriate tool. (DVWA or equivalent tools)	2
11	Configure Firewall for service acquisitions and limitations in Linux environment	4
12	Configure intrusion detection system (IDS) using appropriate tool. (Snort or equivalent tools)	2
13	Perform system log analysis using appropriate tool. (OSSEC or equivalent tools)	2
14	Validate Internet Security Protocols and Applications using appropriate tool (AVISPA or equivalent tools)	4
15	Study of different types of vulnerabilities for hacking a websites / web applications	4
	Total Lab Hours	**48**

Course Designers

1. C.Jeyamala jeyamala@tce.edu
2. M.Thangavel mtit@tce.edu
3. S.Sujtha suju.sujitha@gmail.com

CURRICULUM AND DETAILED SYLLABI

FOR

M.E. COMPUTER SCIENCE AND INFORMATION SECURITY DEGREE PROGRAMME

PROGRAMME ELECTIVES

FOR THE STUDENTS ADMITTED IN THE

ACADEMIC YEAR 2018-19 ONWARDS

THIAGARAJAR COLLEGE OF ENGINEERING
(A Government Aided ISO 9001:2008 certified Autonomous Institution affiliated to Anna University)
MADURAI – 625 015, TAMILNADU

Phone: 0452 – 2482240, 41
Fax: 0452 2483427
Web: www.tce.edu

Passed in Board of Studies Meeting on 14.07.2018 Approved in 56th Academic Council Meeting on 21.7.2018

18ISPA0	SECURITY FOR INTERNET OF THINGS	Category	L	T	P	Credit
		PE	3	0	0	3

Preamble

The course on Security for Internet of Things will examine the security and ethical issues of the vast implementation of smart devices known as the Internet of Things (IoT). The IoT is an environment where smart devices sense, anticipate, and respond to our needs as we manage them remotely. These smart devices often act as the gateway between our digital and physical world. The IoT touches many aspects of life including transportation, health care, safety, environment, energy, and more. This course will examine and discuss IoT technology and market specific topics, relevant case studies of IoT security vulnerabilities and attacks, and mitigation controls.

Prerequisite

None

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bloom's Level	Expected Proficiency	Expected Level of Attainment (in %)
CO1:	Explain the IoT architecture and protocols	Understand	A	70
CO2:	Demonstrate the IoT application framework	Understand	A	70
CO3:	Solve the given problem through various IoT devices and tools	Apply	B	80
CO4:	Apply the vulnerabilities and authentication schemes for the given IoT problem	Apply	B	80
CO5	Examine the given IoT problem through data privacy of security	Analyze	B	70

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1.	M	L									L
CO2.	M	L									L
CO3.	S	M	L		M		M	M	M		M
CO4.	S	M	L		L						L
CO5.	S	S	M	L	M	M	M	M	M	M	M

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	Continuous Assessment Tests			Terminal Examination
	1	2	3	
Remember	20	20	20	20
Understand	40	40	40	40
Apply	40	40	40	40
Analyze	0	0	0	0
Evaluate	0	0	0	0
Create	0	0	0	0

Attainment of Course outcomes CO5 is assessed through case study

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Compare SOA based and API oriented architecture.
2. Explain the message passing technologies used for devices communication.
3. Outline the features of General Architecture of a Stream-Processing System in IoT

Course Outcome 2 (CO2):

4. Demonstrate of a Peer-to-Peer network topology using Coordinator and end device network device types.
5. Demonstrate of Peer-to-Peer communication between Coordinator and end device through Router
6. Establish Many-to-One Communication (Star Network Topology)
7. Establish Tree Network Topology
8. Establish Cluster Tree Network

Course Outcome 3 (CO3):

9. Read Temperature and Relative Humidity value from the sensor.
10. Read Light intensity value from light sensor
11. Read atmospheric pressure value from pressure sensor
12. Proximity detection with IR LED.
13. Generation of alarm through Buzzer

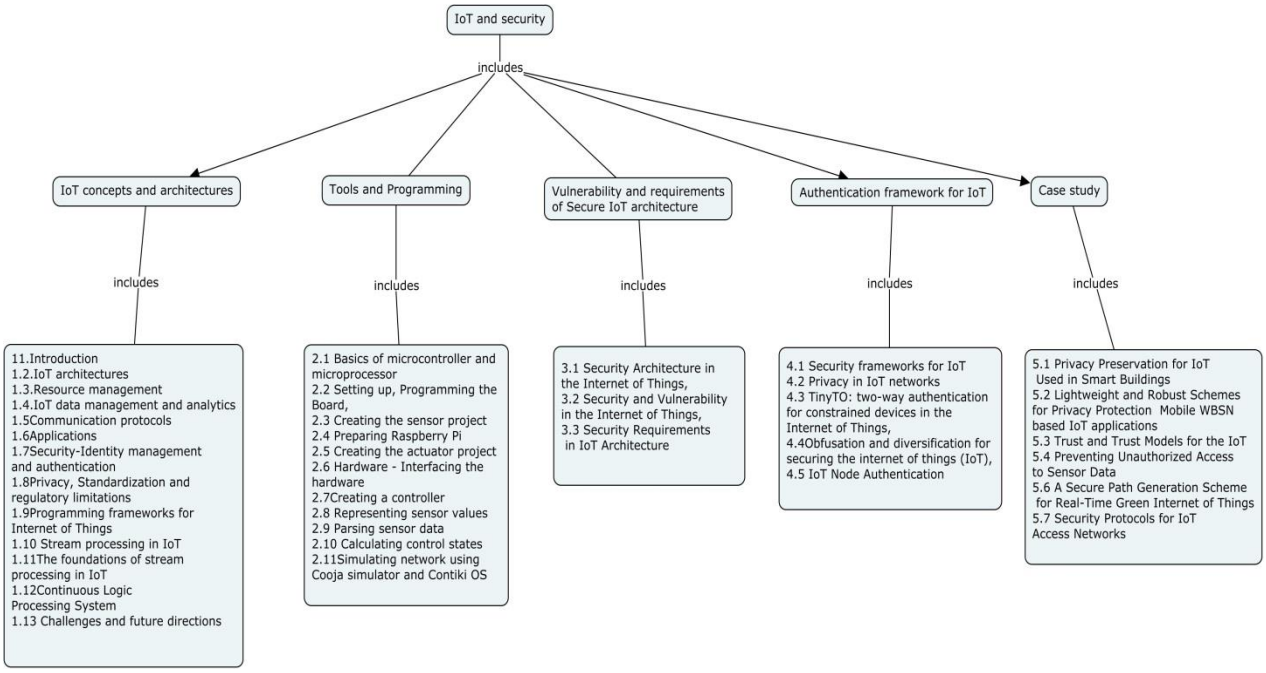
Course Outcome 4 (CO4):

14. Identify the security requirements and vulnerabilities in the Internet of Things (IoT).
15. Experiment with secrecy and secret-key generation in web applications versus the Internet of Things (IoT).
16. Develop the four-layer security architecture of the Internet of Things (IoT)

Course Outcome 5 (CO5):

17. Examine the need of Privacy Preservation for IoT Used in Smart Buildings
18. Inspect the techniques used to Prevent Unauthorized Access in Sensor Data
19. Analyze the Security Protocols for IoT Access Networks.

Concept Map



Syllabus

IoT concepts and architectures: Introduction- IoT architectures-Resource management-IoT data management and analytics-Communication protocols-Applications-Security-Identity management and authentication-Privacy, Standardization and regulatory limitations-Programming frameworks for Internet of Things-Stream processing in IoT-The foundations of stream processing in IoT, Continuous Logic Processing System, Challenges and future directions

Tools and Programming:

Basics of microcontroller and microprocessor -Setting up, Programming the Board, Creating the sensor project - Preparing Raspberry Pi - Creating the actuator project. Hardware - Interfacing the hardware - Creating a controller - Representing sensor values - Parsing sensor data - Calculating control states –Simulating network using Cooja simulator and Contiki OS.

Vulnerability and requirements of Secure IoT architecture: Security Architecture in the Internet of Things, Security and Vulnerability in the Internet of Things, Security Requirements in IoT Architecture.

Authentication framework for IoT: Security frameworks for IoT-Privacy in IoT networks, TinyTO: two-way authentication for constrained devices in the Internet of Things, Obfuscation and diversification for securing the internet of things (IoT), IoT Node Authentication

Case study: Privacy Preservation for IoT Used in Smart Buildings-Lightweight and Robust Schemes for Privacy Protection Mobile WBSN based IoT applications-Trust and Trust Models for the IoT-Preventing Unauthorized Access to Sensor Data-A Secure Path Generation Scheme for Real-Time Green Internet of Things -Security Protocols for IoT Access Networks

References

1. Rajkumar Buyya, Amir Vahid Dastjerdi," Internet of Things Principles and Paradigms",Elsevier , First edition ,2016

2. Fei Hu," Security and Privacy in Internet of Things (IoTs),Models, Algorithms, and Implementations",CRC Press, First edition ,2016.
3. Shancang Li Li Da Xu," Securing the Internet of Things",Elsevier, First edition ,2016
4. Brian Russell, Drew Van Duren," Practical Internet of Things Security", PACKT publishing, First edition, 2016.
5. The Internet of Things: Privacy and Security in a Connected World, Federal Trade Commission staff reports, United States. Federal Trade Commission, DIANE Publishing Company, 2015
6. Fei Hu, "Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations", CRC Press, 2016
7. Sridipta Misra, Muthucumaru Maheswaran, Salman Hashmi, "Security Challenges and Approaches in Internet of Things", Springer, 2016
8. Jeyanthi, N., Thandeeswaran, R., " Security Breaches and Threat Prevention in the Internet of Things", IGI Global, 2017

Course Contents and Lecture Schedule

Module No.	Topic	No. of Lectures
1	**IoT concepts and architectures**	
1.1	Introduction	1
1.2	IoT architectures	
1.3	Resource management	1
1.4	IoT data management and analytics	1
1.5	Communication protocols	1
1.6	Applications	1
1.7	Security-Identity management and authentication	1
1.8	Privacy, Standardization and regulatory limitations	1
1.9	Programming frameworks for Internet of Things	1
1.10	Stream processing in IoT	1
1.11	The foundations of stream processing in IoT	1
1.12	Continuous Logic Processing System	1
1.13	Challenges and future directions	1
2	**Tools and Programming:**	
2.1	Basics of microcontroller and microprocessor	1
2.2	Setting up, Programming the Board,	1
2.3	Creating the sensor project	1
2.4	Preparing Raspberry Pi	1
2.5	Creating the actuator project	1
2.6	Hardware - Interfacing the hardware	1
2.7	Creating a controller	1
2.8	Representing sensor values	1
2.9	Parsing sensor data	1
2.10	Calculating control states	1
2.11	Simulating network using Cooja simulator and Contiki OS	2
3	**Vulnerability and requirements of Secure IoT architecture:**	
.1	Security Architecture in the Internet of Things,	1
3.2	Security and Vulnerability in the Internet of Things,	1

Module No.	Topic	No. of Lectures
3.3	Security Requirements in IoT Architecture	1
4	**Authentication framework for IoT**	
4.1	Security frameworks for IoT	1
4.2	Privacy in IoT networks	1
4.3	TinyTO: two-way authentication for constrained devices in the Internet of Things,	1
4.4	Obfusation and diversification for securing the internet of things (IoT),	1
4.5	IoT Node Authentication	
5	**Case study**	
5.1	Privacy Preservation for IoT Used in Smart Buildings	1
5.2	Lightweight and Robust Schemes for Privacy Protection Mobile WBSN based IoT applications	1
5.3	Trust and Trust Models for the IoT	1
5.4	Preventing Unauthorized Access to Sensor Data	1
5.5	A Secure Path Generation Scheme for Real-Time Green Internet of Things	1
5.6	Security Protocols for IoT Access Networks	
Total Lectures		**36**

Course Designers:

1. .P.Karthikeyan karthikit@tce.edu
2. C.V.Nisha Angeline **nishaangeline@gmail.com**

18ISPB0	MOBILE AND WIRELESS SECURITY	Category	L	T	P	Credit
		PE	3	0	0	3

Preamble

The course follows the evolution of mobile and wireless security, and the underlying principles. The course is designed to educate the purpose of defending systems from unauthorized wireless attacks. This course also discovers the latest security standards and practices in mobile and wireless network.

Prerequisite

Nil

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bloom's Level	Expected Proficiency	Expected Level of Attainment (in %)
CO1:	Explain various wireless technologies, wireless network standards and their threats.	Understand	A	90
CO2:	Identify how hackers and auditors alike test wireless networks for vulnerabilities such as rogue access points, denial of service (DoS) attacks and client-side threats.	Understand	A	90
CO3:	Explain the mobile data network standards and its challenges.	Understand	A	90
CO4:	Discover the vulnerabilities and mis - configurations at wireless transport layer.	Apply	B	80
CO5:	Show how an attacker might attempt to subvert and bypass Wireless security measures in Bluetooth and WiFi.	Apply	B	80
CO6:	Demonstrate various hacking and vulnerability assessment tools to assess the security of wireless and sensor networks, including cracking WEP and WPA security	Apply	B	80

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	M	L									
CO2	M	L									
CO3	M	L									
CO4	M	L		L							
CO5	M	M	L	L							
CO6	S	M	M	L	L			L	M	L	L

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	Continuous Assessment Tests			Terminal Examination
	1	2	3	
Remember	20	20	20	20
Understand	80	40	20	20
Apply	-	40	60	60
Analyse	-	-	-	-
Evaluate	-	-	-	-
Create	-	-	-	-

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Explain in detail about Wired Equivalent Privacy (WEP).
2. Report some of the vulnerabilities susceptible to wireless networks.
3. Identify various attacks in wireless networks.

Course Outcome 2 (CO2):

4. Recognize the following attacks and specify the appropriate actions to take to mitigate vulnerability and risk – DOS and DDOS.
5. Define spoofing. Write various types of spoofing.
6. List the countermeasures of securing the WLAN.

Course Outcome 3 (CO3):

7. Report all security issues in GSM.
8. Identify the countermeasures of securing wireless network.
9. Classify the various wireless device security issues.

Course Outcome 4 (CO4):

10. For the given network topology, analyze the traffic and find out the safe transmission between nodes.
11. Encrypt the data packets sent through Bluetooth using any of the encryption algorithms.
12. Using public key cryptosystems authenticate and encrypt the data transmitted.

Course Outcome 5 (CO5):

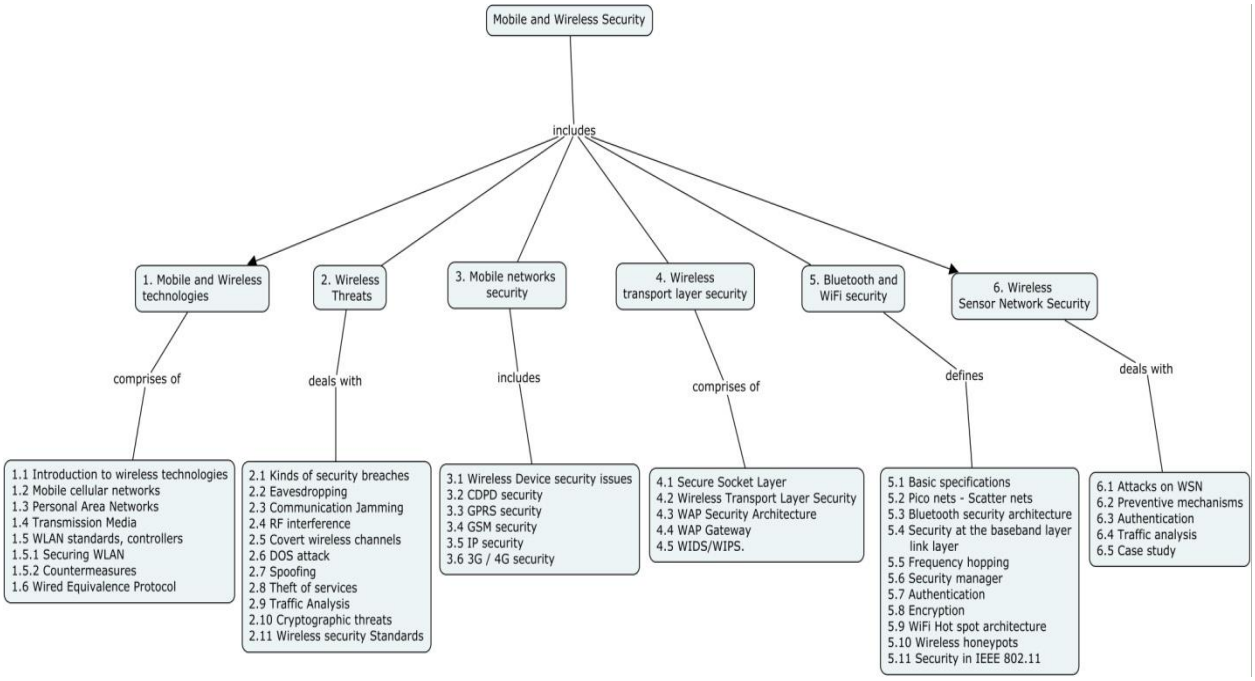
13. Explain the various threads to the wireless sensor networks.
14. Examine the authentication schemes to prevent the attacks on wireless sensor networks.
15. Solve the following case study and provide appropriate solutions,

    Organization: European bank.
    Application: Wireless banking and digital signing.
    Business requirement: To enable wireless banking and signing of transactions from mobile phones. The organization has already a presence on the internet with a web based banking solution and was aggressively it moving toward a wireless edition of the banking application. Provide a solution according to the business requirement.

Course Outcome 6 (CO6):

- **Assessed through Assignment**

Concept Map



Syllabus

Mobile & Wireless technologies: Introduction to wireless technologies - Mobile cellular networks - Personal Area Networks -Transmission Media – WLAN standards, controllers - Securing WLAN - Countermeasures - Wired Equivalence Protocol (WEP).

Wireless threats: Kinds of security breaches - Eavesdropping - Communication Jamming - RF interference - Covert wireless channels - DOS attack – Spoofing - Theft of services - Traffic Analysis-Cryptographic threats - Wireless security Standards.

Mobile networks security: Wireless Device security issues - CDPD security (Cellular Digital Packet Data)-GPRS security (General Packet Radio Service) - GSM (Global System for Mobile Communication) security – IP security - 3G / 4G security.

Wireless transport layer security: Secure Socket Layer - Wireless Transport Layer Security - WAP Security Architecture - WAP Gateway - Wireless Intrusion Detection and Prevention Systems (WIDS/WIPS).

Bluetooth & WiFi security: Basic specifications - Pico nets – Scatter nets - Bluetooth security architecture – Security at the baseband layer and link layer – Frequency hopping – Security manager – Authentication – Encryption - WiFi Hot spot architecture - Wireless honeypots - Security in IEEE 802.11.

Wireless Sensor Network Security
Attacks on wireless sensor network and Preventive mechanisms: authentication and traffic analysis, Case study: centralized and passive intruder detection

Case studies: Case study 1 – Public safety wireless networks, Case study 2 – Satellite communications systems , Case study 3 – Wide Area Wireless Data Services (CDPD, GPRS, etc.), Case study 4 – Wireless LANs (802.11, etc.), Case study 5 – Wireless Metropolitan Area Networks (e.g., 802.16)

Reference Books

1. Wireless and Mobile Network Security-Security basics, Security in On-the-shelf and emerging technologies, Hakima Chaouchi, Maryline Maknavicius, ISBN: 9781848211179, 2010.
2. Wireless Security-Models, Threats and Solutions, Nichols and Lekka, Tata McGraw – Hill, New Delhi, 2006.
3. Wireless Security, Merritt Maxim and David Pollino, Osborne/McGraw Hill, New Delhi, 2005.
4. Mobile and Wireless Network Security and Privacy, Springer, ISBN: 0387710574, edition 2007.
5. Wireless Network Security: Theories and Applications, Springer, ISBN: 978-3642365102, 2013

Course Contents and Lecture Schedule

Module No.	Topic	No. of Lectures
1	**Mobile & Wireless technologies**	
1.1	Introduction to wireless technologies	1
1.2	Mobile cellular networks	
1.3	Personal Area Networks	1
1.4	Transmission Media	1
1.5	WLAN standards, controllers	1
1.5.1	Securing WLAN - Countermeasures	1
1.6	WEP (Wired Equivalence Protocol)	1
2	**Wireless Threats**	
2.1	Kinds of security breaches	1
2.2	Eavesdropping	
2.3	Communication Jamming	1
2.4	RF interference	
2.5	Covert wireless channels	1
2.6	DOS attack – Spoofing	
2.7	Theft of services	1
2.8	Traffic Analysis	
2.9	Cryptographic threats	1
2.10	Wireless security Standards	
3	**Mobile Networks Security**	
3.1	Wireless Device security issues	
3.2	CDPD security (Cellular Digital Packet Data)	1
3.3	GPRS security (General Packet Radio Service)	1
3.4	GSM (Global System for Mobile Communication) security	2
3.5	IP security	1
3.6	3G / 4G security.	1
4	**Wireless Transport Layer Security**	
4.1	Secure Socket Layer	1
4.2	Wireless Transport Layer Security	1
4.3	WAP Security Architecture	2
4.4	WAP Gateway	
4.5	Wireless Intrusion Detection and Prevention Systems (WIDS/WIPS).	
5	**Bluetooth & WiFi Security**	

Module No.	Topic	No. of Lectures
5.1	Basic specifications, Pico nets, Scatter nets	1
5.2	Bluetooth security architecture	1
5.3	Security at the baseband layer and link layer	1
5.4	Frequency hopping, Security manager	1
5.5	Authentication, Encryption	1
5.6	WiFi Hot spot architecture	1
5.7	Wireless honeypots	1
5.8	Security in IEEE 802.11	1
6	**Wireless Sensor Network Security**	
6.1	Attacks on WSN	1
6.2	Preventive mechanisms	
6.3	Authentication	1
6.4	Traffic analysis	
6.5	Case study: Centralized and passive intruder detection	1
7	**Case Studies**	
7.1	Public safety wireless networks	1
7.2	Wide Area Wireless Data Services (CDPD, GPRS, etc.)	1
7.3	Wireless LANs (802.11, etc.)	1
7.4	Wireless Metropolitan Area Networks (e.g., 802.16)	1
Total Lectures		**36**

Course Designers:

1. S.Muthuramalingam smrit@tce.edu
2. M.Manikandakumar mmrit@tce.edu

18ISPCO	SYSTEM SECURITY	Category	L	T	P	Credit
		PE	3	0	0	3

Preamble

This course provides a deep and comprehensive study of the security principles and practices of computer systems. Topics include access control, common attacking techniques, operating system security, software security, database security, web security Privacy protection, Anonymity Services, Trusted computing, Multilevel security and Management issues.

Prerequisite

Nil

Course Outcomes

On successful completion of the course, students will be able to

Course Outcomes		Bloom's Level	Expected Proficiency	Expected Level of Attainment (in %)
CO1	Identify the requirements to implement access control mechanisms for the given system scenario.	Apply	B	85
CO2	Practice the countermeasures for ensuring system security against malicious software, denial of service attacks, and buffer overflow.	Apply	B	85
CO3	Illustrate the security techniques used to protect operating system, software, and database.	Apply	B	80
CO4	Inspect the security essentials in client and service side components of the given system scenario.	Analyze	B	75
CO5	Demonstrate the security of the system with Privacy protection, Anonymity Services, Trusted computing and Multilevel security.	Apply	B	80
CO6	Illustrate appropriate mechanisms for protecting information systems by addressing security management issues.	Apply	B	80

Mapping with Programme Outcomes / Programme Specific Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	S	M	M								
CO2	S	M	M		S		M	L	L		
CO3	S	M	M		S		M	L	L		
CO4	S	S	M		S		M	L	L		
CO5	S	M	M								
CO6	S	M	M								

S - Strong, M – Medium, L – Low

Assessment Pattern

Bloom's Assessment Category	CAT 1	CAT 2	CAT 3	Terminal Exam
Remember	20	10	20	20
Understand	20	20	20	20
Apply	50	60	50	50
Analyze	10	10	10	10
Evaluate	0	0	0	0
Create	0	0	0	0

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Consider user accounts on a system with a Web server configured to provide access to user Web areas. In general, this uses a standard directory name, such as 'public_html', in a user's home directory. This acts as their user Web area if it exists. However, to allow the Web server to access the pages in this directory, it must have at least search (execute) access to the user's home directory, read/execute access to the Web directory, and read access to any Web pages in it. Consider the interaction of this requirement with the cases you discussed for the preceding problem. What consequences does this requirement have? Note that a Web server typically executes as a special user, and in a group that is not shared with most users on the system. Are there some circumstances when running such a Web service is simply not appropriate? Explain.
2. Assume a system with *N* job positions. For job position *i*, the number of individual users in that position is *Ui* and the number of permissions required for the job position is *Pi*.
3. For a traditional DAC scheme, how many relationships between users & permissions must be defined?
4. For a RBAC scheme, how many relationships between users and permissions must be defined?
5. An early attempt to force users to use less predictable passwords involved computer supplied passwords. The passwords were eight characters long and were taken from the character set consisting of lowercase letters and digits. They were generated by a pseudorandom number generator with 2^{15} possible starting values. Using the technology of the time, the time required to search through all character strings of length 8 from a 36-character alphabet was 112 years. Unfortunately, this is not a true reflection of the actual security of the system. Explain the problem.

Course Outcome 2 (CO2):

6. Assume you receive an e-mail, which appears to come from your bank, includes your bank logo in it, and with the following contents: "Dear Customer, Our records show that your Internet Banking access has been blocked due to too many login attempts with invalid information such as incorrect access number, password, or security number. We urge you to restore your account access immediately, and avoid permanent closure of your account, by clicking on this *link to restore your account.* Thank you from your customer service team." What form of attack is this e-mail attempting? What is the most likely mechanism used to distribute this e-mail? How should you respond to such e-mails?

7. In order to implement a DNS amplification attack, the attacker must trigger the creation of a sufficiently large volume of DNS response packets from the intermediary to exceed the capacity of the link to the target organization. Consider an attack where the DNS response packets are 500 bytes in size (ignoring framing overhead). How many of these packets per second must the attacker trigger to flood a target organization using a 0.5-Mbps link? A 2-Mbps link? Or a10-Mbps link? If the DNS request packet to the intermediary is 60 bytes in size, how much bandwidth does the attacker consume to send the necessary rate of DNS request packets for each of these three cases?
8. Investigate the details of the format string overflow attack, how it works, and how the attack string it uses is designed. Then experiment with implementing this attack against a suitably vulnerable test program.

Course Outcome 3 (CO3):

9. Consider an automated audit log analysis tool (e.g., swatch). Can you propose some rules which could be used to distinguish “suspicious activities” from normal user behavior on a system for some organization?
10. Some have argued that Unix/Linux systems reuse a small number of security features in many contexts across the system, while Windows systems provide a much larger number of more specifically targeted security features used in the appropriate contexts. This may be seen as a trade-off between simplicity and lack of flexibility in the Unix/Linux approach, against a better targeted but more complex and harder to correctly configure approach in Windows. Discuss this trade-off as it impacts on the security of these respective systems, and the load placed on administrators in managing their security.
11. Another approach to improving program safety is to use a static analysis tool, which scans the program source looking for known program deficiencies. Identity some suitable static analysis tools for a language that you know. Determine the cost, availability, and ease of use of these tools. Indicate the types of development projects they would be suitable to use in.

Course Outcome 4 (CO4):

12. How to turn off the "You are submitting the contents of a form insecurely" message in Netscape? Need to worry about it?
13. How secure is the encryption used by SSL?
14. When the user try to view a secure page, the browser complains that it doesn't recognize the authority that signed its certificate and asks the user want to continue. What the user need to do?
15. Are there any known security holes in JavaScript?
16. Do "Cookies" Pose any Security Risks?

Course Outcome 5 (CO5):

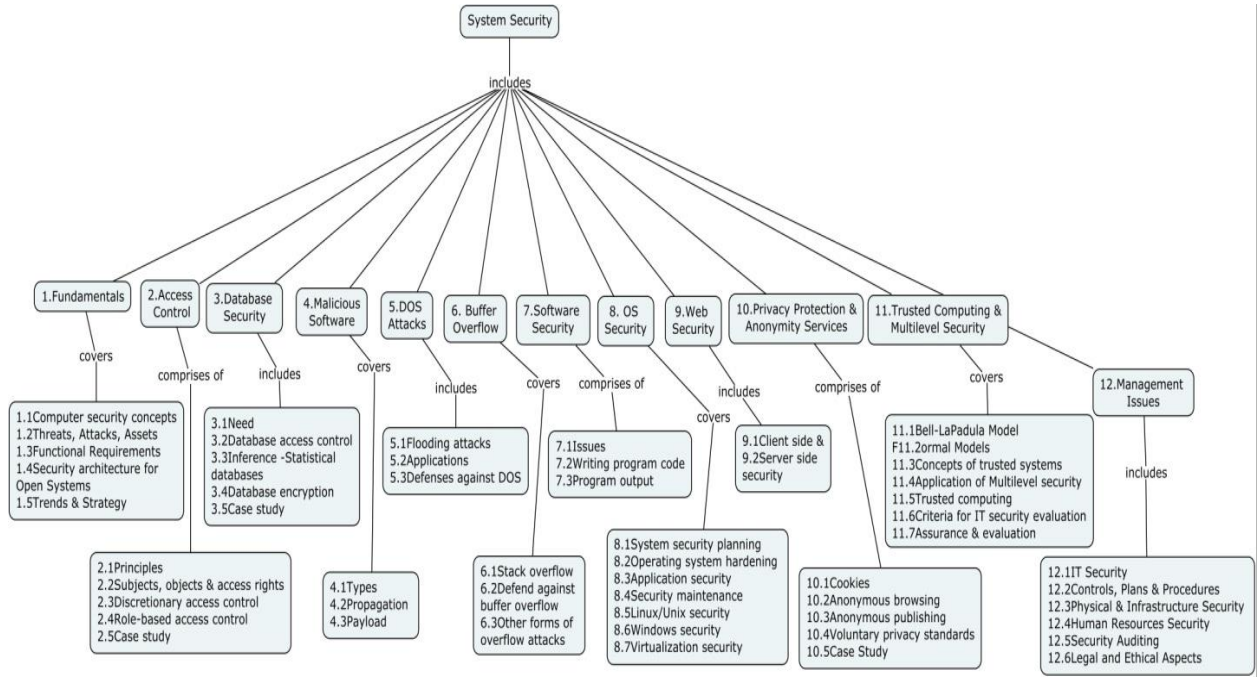
17. When you review the list of products evaluated against the Common Criteria, such as that found on the Common Criteria Portal Web site, very few products are evaluated to the higher EAL 6 and EAL 7 assurance levels. Indicate why the requirements of these levels limit the type and complexity of products that can be evaluated to them. Do you believe that a general-purpose operating system, or database management system, could be evaluated to these levels?

18. Investigate whether your country has a government agency that manages Common Criteria product evaluations. Locate the Web site for this function, and then find the list of Evaluated/Verified Products endorsed by this agency. Alternatively, locate the list on the Common Criteria Portal site.
    - Each of the following descriptions applies to one or more of the rules in the Clark-Wilson model. Identify the rules in each case.
    - Provide the basic framework to ensure internal consistency of the CDIs.
    - Provide a mechanism for external consistency that control which persons can execute which programs on specified CDIs. This is the separation of duty mechanism.
    - Provide for user identification.
    - Maintain a record of TPs.
    - Control the use of UDIs to update or create CDIs.
    - Make the integrity enforcement mechanism mandatory rather then discretionary.

Course Outcome 6 (CO6):

19. As part of a formal risk assessment on the use of laptops by employees of a large government department, you have identified the asset “confidentiality of personnel information in a copy of a database stored unencrypted on the laptop” and the threat “theft of personal information, and its subsequent use in identity theft caused by the theft of the laptop.” Suggest reasonable values for the items in the risk register for this asset and threat, and provide justifications for your choices.
20. Phil maintains a blog online. What do you do to check that his blog is not revealing sensitive company information? Is he allowed to maintain his blog during work hours? He argues that his blog is something he does when not at work. How do you respond? You discover that his blog contains a link to the site Your Company Sucks. Phil states he is not the author of that site. Now what do you do?
21. As part of a formal risk assessment of desktop systems in a small accounting firm with limited IT support, you have identified the asset “integrity of customer and financial data files on desktop systems” and the threat “corruption of these files due to import of a worm/virus onto system.” Suggest reasonable values for the items in the risk register for this asset and threat, and provide justifications for your choices.

Concept Map



Syllabus

Fundamentals: Computer security concepts - Threats, Attacks, Assets - Functional requirements - Security architecture - Trends - Strategy.

Access Control: Principles - Subjects, objects and access rights - Discretionary access control - Role-based access control - Case study: UNIX file access control, RBAC system for Bank, Iris biometric system, Security problems in ATM systems.

Database Security: Need - DBMS - Relational databases - Database access control - Inference - Statistical databases - database encryption - Case study: Cloud security.

Malicious software: Types of Malware - Propagation : Infected content, Vulnerability Exploit, SPAM E-mail, Trojans - Payload : System corruption, Attack agent, Information theft, Stealthing – Countermeasures.

Denial of Service Attacks: Flooding attacks - Distributed Denial of Service attacks - Application-based Bandwidth attacks - Reflector and Amplifier attacks - Defenses against DoS - Responding to DoS.

Buffer overflow: Stack overflow - Defend against buffer overflow - Other forms of overflow attacks.

Software security: Issues - Handling program input - Writing safe program code - Interacting with the operating systems and other programs - Handling program output.

Operating system security: System security planning - Operating system hardening - Application security - Security maintenance - Linux/Unix security - Windows security - Virtualization security.

Web Security: Client-side security - Binary mail attachments - Helper applications and plug-ins - Scripting languages - Java Applets - Active X controls - Security zones - Implications for firewalls. Server-side security - CGI - Server APIs - FastCGI - Server-side Includes - ASP - JSP.

Privacy Protection and Anonymity Services: Cookies - Anonymous browsing - Anonymous publishing - Voluntary privacy standards - Case Study: Security and Privacy issues in Big Data, IoT and Cloud Computing..

Trusted computing and Multilevel security: Bell-LaPadula Model - Formal Models - Concepts of trusted systems - Application of Multilevel security - Trusted computing and Trusted platform module - Criteria for IT security evaluation - Assurance and evaluation.

Management Issues: IT Security management and risk assessment - Controls, Plans and Procedures - Physical and Infrastructure Security - Human Resources Security - Security Auditing - Legal and Ethical Aspects.

Text Books

1. William Stallings, Lawrie Brown, " Computer Security: Principles and Practice" Pearson, Fourth edition, 2017.
2. James Michael Stewart, Mike Chapple, Darril Gibson, " Certified Information Systems Security Professional Study Guide", John Wiley & Sons, Seventh Edition, 2015.

References

1. David Kim and Michael Solomon, "Fundamentals of Information System Security", Jones & Bartlett Learning, Third Edition, 2018
2. M. Stamp, “Information Security: Principles and Practice,”, Wiley,2nd Edition,2011.
3. M. E. Whitman and H. J. Mattord, “Principles of Information Security,” 4th Edition, 2011.
4. Bernard Menezes, “Network Security and Cryptography”, Cengage Learning India,1st Edition,2010.
5. G. McGraw, “Software Security: Building Security In,” Addison Wesley, 2006.
6. M. Bishop, “Computer Security: Art and Science,” Addison Wesley, 2002.
7. Rolf Oppliger, " Security Technologies for the World Wide Web", Artech House Computer Security Series, Second edition, 2002.

Course Contents and Lecture Schedule

Module No	Topic	No. of Lecture Hours
1	Fundamentals	
1.1	Computer security concepts	1
1.2	Threats, Attacks, Assets	
1.3	Functional Requirements	1
1.4	Security architecture for Open Systems	
1.5	Trends & Strategy	
2	Access Control	
2.1	Principles	1
2.2	Subjects, objects and access rights	
2.3	Discretionary access control	1
2.4	Role-based access control	
2.5	Case study: UNIX File access control, RBAC system for Bank.	1
3	Database Security	
3.1	Need - DBMS - Relational databases	1

Module No	Topic	No. of Lecture Hours
3.2	Database access control	1
3.3	Inference - Statistical databases	1
3.4	Database encryption	
3.5	Case study: Cloud security.	
4	Malicious Software	
4.1	Types of Malware	2
4.2	Propagation : Infected content, Vulnerability Exploit, SPAM E-mail, Trojans	
4.3	Payload : System corruption, Attack agent, Information theft, Stealthing	1
5	Denial of Service Attacks	
5.1	Flooding attacks - Distributed Denial of Service attacks	1
5.2	Application-based Bandwidth attacks - Reflector and Amplifier attacks	1
5.3	Defenses against DoS - Responding to DoS.	1
6	Buffer Overflow	
6.1	Stack overflow	2
6.2	Defend against buffer overflow	
6.3	Other forms of overflow attacks	
7	Software Security	
7.1	Issues - Handling program input	2
7.2	Writing safe program code	
7.3	Interacting with the operating systems and other programs - Handling program output	
8	Operating System Security	
8.1	System security planning	1
8.2	Operating system hardening	
8.3	Application security	1
8.4	Security maintenance	
8.5	Linux/Unix security	1
8.6	Windows security	
8.7	Virtualization security	
9	Web Security	
9.1	Client-side security - Binary mail attachments - Helper applications and plug-ins - Scripting languages - Java Applets - Active X controls - Security zones - Implications for firewalls.	2
9.2	Server-side security - CGI - Server APIs - FastCGI - Server-side Includes - ASP - JSP.	2
10	Privacy Protection and Anonymity Services	
10.1	Cookies	1
10.2	Anonymous browsing	
10.3	Anonymous publishing	
10.4	Voluntary privacy standards	
10.5	Case Study: Security and Privacy issues in Big Data, IoT and Cloud Computing..	1
11	Trusted computing and Multilevel security	
11.1	Bell-LaPadula Model	1
11.2	Formal Models	
11.3	Concepts of trusted systems	

Module No	Topic	No. of Lecture Hours
11.4	Application of Multilevel security	1
11.5	Trusted computing and Trusted platform module	
11.6	Criteria for IT security evaluation	1
11.7	Assurance and evaluation	
12	**Management Issues**	
12.1	IT Security management and risk assessment	1
12.2	Controls, Plans and Procedures	1
12.3	Physical and Infrastructure Security	1
12.4	Human Resources Security	1
12.5	Security Auditing	1
12.6	Legal and Ethical Aspects.	1
Total Hours		36

Course Desginers

1. M.Thangavel mtit@tce.edu
2. .R.Parkavi rpit@tce.edu

CURRICULUM AND DETAILED SYLLABI

FOR

M.E. COMPUTER SCIENCE AND INFORMATION SECURITY DEGREE PROGRAMME

FOR THE STUDENTS ADMITTED IN THE

ACADEMIC YEAR 2018-19 ONWARDS

THIAGARAJAR COLLEGE OF ENGINEERING
(A Government Aided ISO 9001:2008 certified Autonomous Institution affiliated to Anna University)
MADURAI – 625 015, TAMILNADU

Phone: 0452 – 2482240, 41
Fax: 0452 2483427
Web: www.tce.edu

Passed in Board of Studies Meeting on 08.12.2018 Approved in 57th Academic Council Meeting on 5.01.2019

THIAGARAJAR COLLEGE OF ENGINEERING
DEPARTMENT OF INFORMATION TECHNOLOGY

VISION

Evolve into a **Centre of Excellence for Education and Research** in Information Technology.

MISSION

- Attaining academic excellence through well designed curriculum adaptable to dynamic technological needs, competent faculty and innovative teaching-learning process.
- Promoting collaborative research through special interest groups, state of the art research labs Industry Institute interactions
- Facilitating value added courses to produce highly competent and socially conscious information technology professionals and entrepreneurs.

PROGRAM EDUCATIONAL OBJECTIVES

Graduates of the programme will

PEO 1 Contribute effectively to serve the society through information security enabled solutions and products adhering to professional ethics and cyber laws.

PEO 2 Articulate fundamental concepts, design underpinnings of information security, and research findings to train professionals or to educate engineering students.

PEO 3 Ppursue academic research in Information Security and contribute significantly in the field of Computer science.

PEO 4 Engage in lifelong learning to adapt to changing technological needs for career advancement.

PROGRAM OUTCOMES

PO1 Scholarship of Knowledge

Acquire in-depth knowledge of specific discipline or professional area, including wider and global perspective, with an ability to discriminate, evaluate, analyse and synthesize existing and new knowledge, and integration of the same for enhancement of knowledge.

PO2 Critical Thinking

Analyse complex engineering problems critically, apply independent judgment for synthesizing information to make intellectual and/or creative advances for conducting research in a wider theoretical, practical and policy context.

PO3 Problem Solving

Think laterally and originally, conceptualize and solve engineering problems, evaluate a wide range of potential solutions for those problems and arrive at feasible, optimal solutions after considering public health and safety, cultural, societal and environmental factors in the core areas of expertise.

PO4 Research Skill

Extract information pertinent to unfamiliar problems through literature survey and experiments, apply appropriate research methodologies, techniques and tools, design, conduct experiments, analyse and interpret data, demonstrate higher order skill and view things in a broader perspective, contribute individually/in group(s) to the development of scientific/technological knowledge in one or more domains of engineering.

PO5 Usage of modern tools

Create, select, learn and apply appropriate techniques, resources, and modern engineering and IT tools, including prediction and modeling, to complex engineering activities with an understanding of the limitations.

PO6 Collaborative and Multidisciplinary work

Possess knowledge and understanding of group dynamics, recognise opportunities and contribute positively to collaborative-multidisciplinary scientific research, demonstrate a capacity for self-management and teamwork, decision-making based on open-mindedness, objectivity and rational analysis in order to achieve common goals and further the learning of themselves as well as others.

PO7 Project Management and Finance

Demonstrate knowledge and understanding of engineering and management principles and apply the same to one's own work, as a member and leader in a team, manage projects efficiently in respective disciplines and multidisciplinary environments after consideration of economical and financial factors.

PO8 C**ommunication**

Communicate with the engineering community, and with society at large, regarding complex engineering activities confidently and effectively, such as, being able to comprehend and write effective reports and design documentation by adhering to appropriate standards, make effective presentations, and give and receive clear instructions.

PO9 Life-long Learning

Recognize the need for, and have the preparation and ability to engage in life-long learning independently, with a high level of enthusiasm and commitment to improve knowledge and competence continuously.

PO10 Ethical Practices and Social Responsibility

Acquire professional and intellectual integrity, professional code of conduct, ethics of research and scholarship, consideration of the impact of research outcomes on professional practices and an understanding of responsibility to contribute to the community for sustainable development of society.

PO11 Independent and Reflective Learning

Observe and examine critically the outcome s of one's actions and make corrective measures subsequently, and learn from mistakes without depending on external feedback.

M.E./M.Tech Programme Structure (CBCS)

Credit Distribution:

S.No	Category		Credits
A.	**Foundation Course**		**3 - 6**
B.	**Programme Core Courses***		**19 – 25**
C.	**Elective Courses**		**17 – 23**
	a.	Programme Elective	15 – 21
	b.	Open Elective	2 – 6
D.	**Common Core Course**		**2**
E.	**Mini Project and Dissertation**		**27**
E	Value Added Courses (Not to be included in CGPA) - Mandatory		**4**
	Minimum Credits to be earned for the award of the degree		**68** (from A to E) and 4 (from F)

*TCP and Laboratory courses are Mandatory in the Programme Core Courses.

Credit Details:

Theory: 3 Credits

Theory Cum Practical (TCP) : 3 Credits,

Lab: 2 Credits

Open Elective: 2 Credits

Mini Project: 2 Credits

Dissertation Phase I: 10 Credits

Dissertation Phase I: 15 Credits

Common Core: Research Methodology and IPR: 2 Credits

Scheduling of Courses

Semester	**Theory**					**Theory Cum Practical**	**Laboratory**	**Project**
I (17)	18IS110 Mathematics for Information Sciences (3 Credits)	18IS120 Distributed and Cloud Computing (3 Credits)	18IS130 Cryptography and Network Security (3 Credits)	18ISPX0 Prog. Elective 1 (3 Credits)	-	18IS160 Algorithm Design Techniques (3 Credits)	18IS170 Cryptography and Network Security Lab (2 Credits)	-
II (21)	18IS210 Ethical Hacking and Cyber Forensics (3 Credits)	18ISPX0 Prog. Elective 2 (3 Credits)	18ISPX0 Prog. Elective 3 (3 Credits)	18ISPX0 Prog. Elective 4 (3 Credits)	18PG250 Common Core (2 Credits)	18IS260 Data Analytics (3 Credits)	18IS270 Ethical Hacking and Cyber Forensics Lab (2 Credits)	18IS280 Mini Project (2 Credits)
III (15)	18ISPX0 Prog. Elective 5 (3 Credits)	-	-	-	18PGPX0 Open Elective (2 Credits)	-	-	18IS380 Dissertation Phase I (10 Credits)
IV (15)	-	-	-	-	-	-	-	18IS480 Dissertation Phase II (15 Credits)

Passed in Board of Studies Meeting on 08.12.2018 Approved in 57th Academic Council Meeting on 5.01.2019

List of Electives

Programme Elective 1:

- Security with Internet of Things
- Mobile and Wireless Security
- Secure Software Engineering
- Advanced Cryptography
- Biometrics
- Cloud Security
- Cyber Physical Systems
- Database Security and Access control
- Identity and Access Management
- Malware Analysis
- Security Assessment and Risk Analysis
- Secure Coding Practices
- Secure Network Management
- Steganography and Digital watermarking
- System Security

Programme Elective 2:

- Artificial Intelligence
- Augmented Reality
- Cognitive Science
- Data Sciences
- Deep Learning
- Enterprise Computing
- Information Theory and Coding
- IT Audit and Control
- Software Defined Networks
- Soft Computing

THIAGARAJAR COLLEGE OF ENGINEERING: MADURAI – 625 015
M.E (Computer Science and Information Security) Degree Programme

COURSES OF STUDY
(For the candidates admitted from 2018-19 onwards)

SECOND SEMESTER

Course Code	Name of the Course	Category	No. of Hours / Week			credits
			L	T	P	
THEORY						
18IS210	Ethical Hacking and Cyber Forensics	PC	3	-	-	3
18ISPX0	Elective- I	PE	3	-	-	3
18ISPX0	Elective- II	PE	3	-	-	3
18ISPX0	Elective- III	PE	3	-	-	3
18PG250	RESEARCH METHODOLOGY AND IPR	CC	2	-	-	2
THEORY CUM PRACTICAL						
18IS260	Data Analytics	PC	2	-	2	3
PRACTICAL						
18IS270	Ethical Hacking and Cyber Forensics Lab	PC	-	-	2	2
18IS280	Mini Project	PC	-	-	2	2
AUDIT COURSES						
18PGAA0	Professional Authoring	AC	-	-	2	2
18PGAB0	Value Education	AC	-	-	2	2
Total			**18**	**-**	**8**	**23**

PC : Program Core
PE : Program Elective
CC : Common Core
AC : Audit Course
OE : Open Elective
Note: L : Lecture T : Tutorial P : Practical
1 Hour Lecture is equivalent to 1 credit

2 Hours Tutorial is equivalent to 1 credit

2 Hours Practical is equivalent to 1 credit

THIAGARAJAR COLLEGE OF ENGINEERING: MADURAI – 625 015
M.E (Computer Science and Information Security) Degree Programme

SCHEME OF EXAMINATIONS
(For the candidates admitted from 2018-19 onwards)

SECOND SEMESTER

S.No.	Course Code	Name of the Course	Duration of Terminal Exam. in Hrs.	Marks			Minimum Marks for Pass	
				Continuous Assessment *	Terminal Exam **	Max. Marks	Terminal Exam	Total
THEORY								
1	18IS210	Ethical Hacking and Cyber Forensics	3	50	50	100	25	50
2	18ISPX0	Elective- I	3	50	50	100	25	50
3	18ISPX0	Elective- II	3	50	50	100	25	50
4	18ISPX0	Elective- III	3	50	50	100	25	50
5	18PG250	Research Methodology And IPR	3	50	50	100	25	50
THEORY CUM PRACTICAL								
6.	18IS260	Data Analytics	3	50	50	100	25	50
PRACTICAL								
7	18IS270	Ethical Hacking and Cyber Forensics Lab	3	50	50	100	25	50
8	18IS280	Mini Project	-	50	50	100	25	50
AUDIT COURSES								
9	18PGAA0	Professional Authoring	-	100	-	100	-	50
10	18PGAB0	Value Education	-	50	50	100	25	50

* CA evaluation pattern will differ from course to course and for different tests. This will have to be declared in advance to students. The department will put a process in place to ensure that the actual test paper follow the declared pattern.

** Terminal Examination will be conducted for maximum marks of 100 and subsequently be reduced to 50 marks for the award of terminal examination marks

18IS210	ETHICAL HACKING AND CYBERFORENSICS	Category	L	T	P	Credit
		PC	3	0	0	3

Preamble

This course provides a detailed knowledge on deployment of security tools and techniques protect computer network. It also covers cyber forensic investigation, including data recovery and security systems design.

Prerequisite

- 18IS130 Cryptography and Network Security

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcome		Blooms Level	Expected Proficiency	Expected level of attainment (%)
CO1:	Explain the security threats and vulnerabilities of a Computer Network.	Understand	A	90
CO2:	Utilize various hacking techniques at system and network level to perform security analysis.	Apply	B	75
CO3:	Use penetration testing tools like Kali Linux to analyze the security level of any network	Analyze	B	75
CO4:	Select suitable countermeasures to protect the network against identified threats	Analyze	B	70
CO5:	Practice the procedure in computer forensics to retrieve evidences for cases in criminal investigations.	Apply	B	75
CO6:	Demonstrate experience in using computer forensic tools like Autopsy and FAW(Forensic Acquisition of Websites)	Apply	B	75

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1.	M	L								S	
CO2.	S	M	M		S			M		S	M
CO3.	S	S	S	M	S	M		M		S	M
CO4.	S	S	S	M	M		L	M	M	S	M
CO5.	S	M	M		M			L		S	
CO6.	S	M	M	M	S	M		M	M	S	M

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	Continuous Assessment Tests			Terminal Examination
	1	2	3	
Remember	20	10	10	10
Understand	30	20	20	20
Apply	50	50	50	50
Analyse	-	20	20	20
Evaluate	-	-	-	-
Create	-	-	-	-

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Discuss briefly about the methodologies to collect information from websites, Regional Internet Registries databases and Networks.
2. Describe briefly, how to enumerate the user accounts and devices on a target computer using an application layer protocol that runs on UDP, and which is used to maintain and manage routers, hubs, and switches on an IP network.
3. Outline the different types of techniques used to identify the open ports on a targeted server or host.
4. Compare the various types of attacks in the process of monitoring and capturing all data packets passing through a given network using software (an application) or hardware device.

Course Outcome 2 (CO2):

1. From the given information, can you identify hosts, ports, and services in a network? Apply in the TCE IT Department Lab network environment and justify your answer.
    i. Establishing the connection between protocols.
    ii. Use fragmented probe packets that reassemble once that reach the targeted host
2. Illustrate how to safeguard the TCE IT Department Lab network from inside and outside attacks by preparing a document or set of documents that describes the security controls, which can be implemented in the lab at a high level.
3. Illustrate with neat sketch, how the attacker perform DOS attacks on a computer or a network by any 4 techniques

Course Outcome 3 (CO3):

1. Sequence and prepare the report for tools as an ethical hacker to identify system attack points and perform password attacks to gain unauthorized access to information system resources.
2. Perform Penetration testing and defend against buffer overflow attacks for a college website
3. Sequence and prepare the report for tools as an ethical hacker to determine organization's publicly available information on the Internet such as network architecture, operating systems, applications, and users

Course Outcome 4 (CO4):

1. Demonstrate how the procedures for changing attacker IP address so that attacker appears to be someone else can be detected and provide any 2 appropriate countermeasures.

2. Apply the wireless encryption standards (WEP, WAP and WAP2) for protecting the TCE-Wifi networks from attackers, who collects sensitive information by breaching the Radio frequency traffic.
3. "At present, most businesses use email as the major source of communication as it is simple and easy to communicate or share information. These emails may contain sensitive information about their projects, updates, etc. If this information falls in to the wrong hands, then the organizations may face huge losses." - Determine security mechanisms to avoid the risk faced by the business organizations

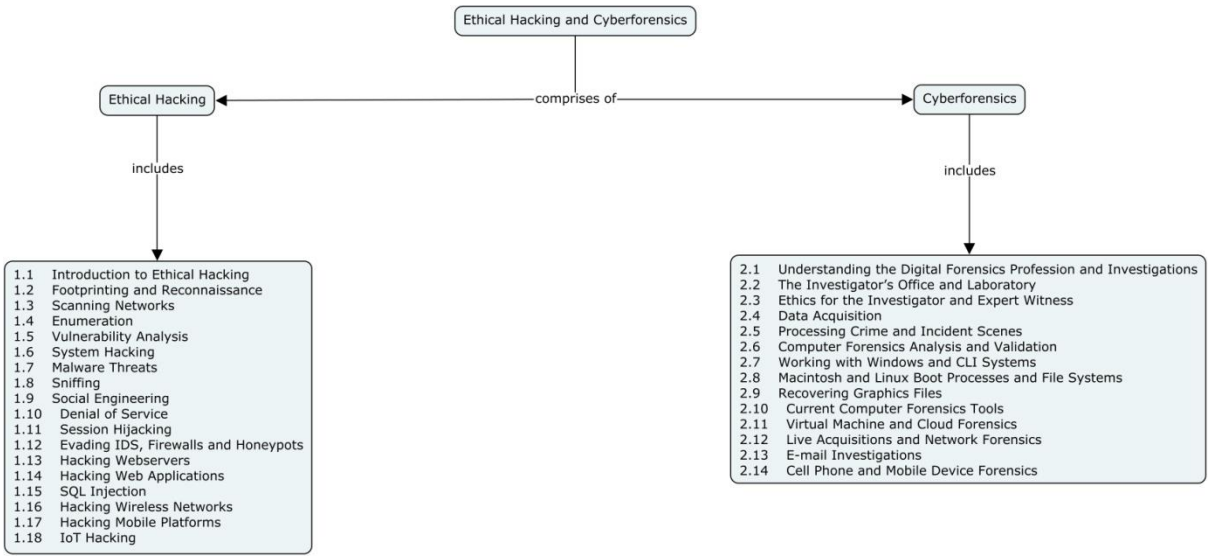
Course Outcome 5 (CO5):

1. In computer forensics,
    i. Distinguish between Identity theft and Identity Fraud.
    ii. Outline the features and problems of Traditional computer crime.
2. Illustrate the different types of computer forensics with traditional systematic approach of computer investigations
3. Demonstrate the essential and methods to analyze and validate the digital evidence.
4. Infer the ways to determine the best data acquisition method for Cyber Investigation.

Course Outcome 6 (CO6):

1. Identify the various data acquisition methods with forensic tools to transfer the digital evidence for forensic analysis
2. Articulate the procedures to acquire logs or screenshots of attackers tasks from cell phone and mobile devices
3. As a Cyber forensic investigator, examine the roles, tasks and tools for investigating Lottery Winner - forgery email

Concept Map



Syllabus

Ethical Hacking:

Basics: Introduction to Ethical Hacking - Footprinting and Reconnaissance -Scanning Networks -Enumeration -Vulnerability Analysis.

System Hacking: System Hacking -Malware Threats -Sniffing -Social Engineering -Denial-of-Service -Session Hijacking.

Network Hacking: Evading IDS, Firewalls, and Honeypots -Hacking Web Servers -Hacking Web Applications -SQL Injection -Hacking Wireless Networks - Hacking Mobile Platforms - IoT Hacking

Cyber Forensics:
Introduction: Understanding the Digital Forensics Profession and Investigations - The Investigator's Office and Laboratory - Ethics for the Investigator and Expert Witness.

Forensic Investigation Process: Data Acquisition - Processing Crime and Incident Scenes - Computer Forensics Analysis and Validation.

Forensic Tools: Working with Windows and CLI Systems - Macintosh and Linux Boot Processes and File Systems - Recovering Graphics Files - Current Computer Forensics Tools

Case Study: Virtual Machine and Cloud Forensics - Live Acquisitions and Network Forensics - Email investigations - Cell Phone and Mobile Device Forensics – Internal / External Hard disk Forensics.

References

1. CEH v10: EC-Council Certified Ethical Hacker Complete Training Guide with Practice Labs: Exam: 312-50, IP Specialist, 2018
2. Bill Nelson, Amelia Phillips, Christopher Steuart, "Guide to Computer Forensics and Investigations", 5th Edition, Delmar Cengage Learning, 2016.
3. Sharma Himanshu, "Kali Linux - An Ethical Hacker's Cookbook", Packt Publishing Limited, 2017
4. Michael Gregg, "CEH Certified Ethical Hacker Version 9: Cert Guide", Second Edition, Pearson, 2017
5. Kenneth C.Brancik "Insider Computer Fraud" Auerbach Publications Taylor & Francis Group–2008.
6. John R. Vacca, "Computer Forensics: Computer Crime Scene Investigation", 2nd Edition, CharlesRiver Media, 2008.

Course Contents and Lecture Schedule

Module No.	Topic	No. of Lecture Hours
1	**Ethical Hacking**	
1.1	Introduction to Ethical Hacking	1
1.2	Footprinting and Reconnaissance	2
1.3	Scanning Networks	2
1.4	Enumeration	1
1.5	Vulnerability Analysis	1
1.6	System Hacking	1
1.7	Malware Threats	1
1.8	Sniffing	1
1.9	Social Engineering	1
1.10	Denial of Service	1
1.11	Session Hijacking	1

Module No.	Topic	No. of Lecture Hours
1.12	Evading IDS, Firewalls and Honeypots	1
1.13	Hacking Webservers	1
1.14	Hacking Web Applications	2
1.15	SQL Injection	1
1.16	Hacking Wireless Networks	1
1.17	Hacking Mobile Platforms	2
1.18	IoT Hacking	1
2	**Cyber Forensics**	
2.1	Understanding the Digital Forensics Profession and Investigations	2
2.2	The Investigator's Office and Laboratory	1
2.3	Ethics for the Investigator and Expert Witness	1
2.4	Data Acquisition	2
2.5	Processing Crime and Incident Scenes	1
2.6	Computer Forensics Analysis and Validation	1
2.7	Working with Windows and CLI Systems	1
2.8	Macintosh and Linux Boot Processes and File Systems	1
2.9	Recovering Graphics Files	1
2.10	Current Computer Forensics Tools	1
2.11	Virtual Machine and Cloud Forensics	1
2.12	Live Acquisitions and Network Forensics	1
2.13	E-mail Investigations	1
2.14	Cell Phone and Mobile Device Forensics - Internal / External Hard disk Forensics	1
	Total Lectures	**36**

Course Designers:

1. C. Jeyamala jeyamala@tce.edu
2. M. Thangavel mtit@tce.edu

18PG250	RESEARCH METHODOLOGY AND IPR

Category	L	T	P	Credit
CC	2	0	0	2

Preamble

The course on the Research Methodology and IPR is offered as common Core course. The objective of this course is to understand and analyze Research Methodology and IPR protection.

Prerequisite

NIL

Course Outcomes

On the successful completion of the course, students will be able to

1. Understand research problem formulation.
2. Analyze research related information
3. Follow research ethics
4. Understand that today's world is controlled by Computer, Information Technology, but tomorrow world will be ruled by ideas, concept, and creativity.
5. Understanding that when IPR would take such important place in growth of individuals & nation, it is needless to emphasis the need of information about Intellectual Property Right to be promoted among students in general & engineering in particular.
6. Understand that IPR protection provides an incentive to inventors for further research work and investment in R&D, which leads to creation of new and better products, and in turn brings about, economic growth and social benefits.

Assessment Pattern

Bloom's Category	Continuous Assessment Tests			End Semester Examination
	1	2	3	
Remember	20	20	20	20
Understand	40	40	40	40
Apply	40	40	40	40
Analyse	0	0	0	0
Evaluate	0	0	0	0
Create	0	0	0	0

Syllabus

Module 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

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

Module 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

Module 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.

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

Module 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

Reference Books

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

Course Designers:

1. Adapted from AICTE Model Curriculum for Postgraduate Degree Courses in Engineering & Technology, Volume-I, January 2018.

		Category	L	T	P	Credit
18IS260	**DATA ANALYTICS (T/P)**	PC	2	0	2	3

Preamble

The course on Data Analytics aims to emphasize the need for and provide an in depth coverage of various analytics techniques. This course aims at facilitating the student to understand the various functionalities of Data Analytics and perform many operations related to creating, using and maintaining databases for Real-world applications and emerging technologies in Data Analytics.

Prerequisite

- Nil

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bloom's Level	Expected Proficiency	Expected level of attainment (%)
Theory				
CO1:	Summarize the workflow of analytics process model, its requirements and applications.	Understand	B	85
CO2:	Apply suitable data pre-processing techniques for the given dataset.	Apply	B	85
CO3:	Demonstrate different predictive, Descriptive and text analytic models.	Apply	B	85
CO4:	Examine Survival Analysis model and learn through Social Network Analytics.	Apply	B	85
Practical				
CO5:	Illustrate and experiment for various data pre-processing techniques, such as missing value estimation, outlier detection and revamping, data standardization and categorization.	Apply	B	85
CO6:	Experiment for different predictive, descriptive and survival analytic models	Analyse	B	80
CO7:	Investigate text and social media analytics for unstructured real time data.	Analyse	B	80

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1.	**L**	**L**							**L**		
CO2.	**L**	**L**	**L**		**M**				**L**	**L**	
CO3.	**M**	**L**	**L**		**S**			**M**	**M**	**M**	
CO4.	**S**	**M**	**M**	**L**	**S**	**L**		**L**	**M**	**M**	
CO5.	**L**	**L**	**L**		**L**				**L**	**L**	
CO6.	**M**	**L**	**L**		**S**			**M**	**M**	**M**	
CO7.	**S**	**M**	**M**	**L**	**S**	**L**		**L**	**M**	**M**	

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	Continuous Assessment Tests			Practical Test	Terminal Examination
	1	2	3		
Remember	30	20	0		0
Understand	30	30	30	30	30
Apply	20	30	50	50	50
Analyse	20	20	20	20	20
Evaluate	0	0	0		0
Create	0	0	0		0

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Identify the requirements of an analytics process model.
2. Describe the Analytics process model.
3. Mention some of the data analytics applications.

Course Outcome 2 (CO2):

1. Compute the technique of sampling and pre-processing for the data set of a bank application. Identify the fields and labels over the dataset and perform all the steps over pre-processing technique.
2. Differentiate among sampling and data pre-processing.
3. Explain the process of filling in the missing values in data pre-processing.

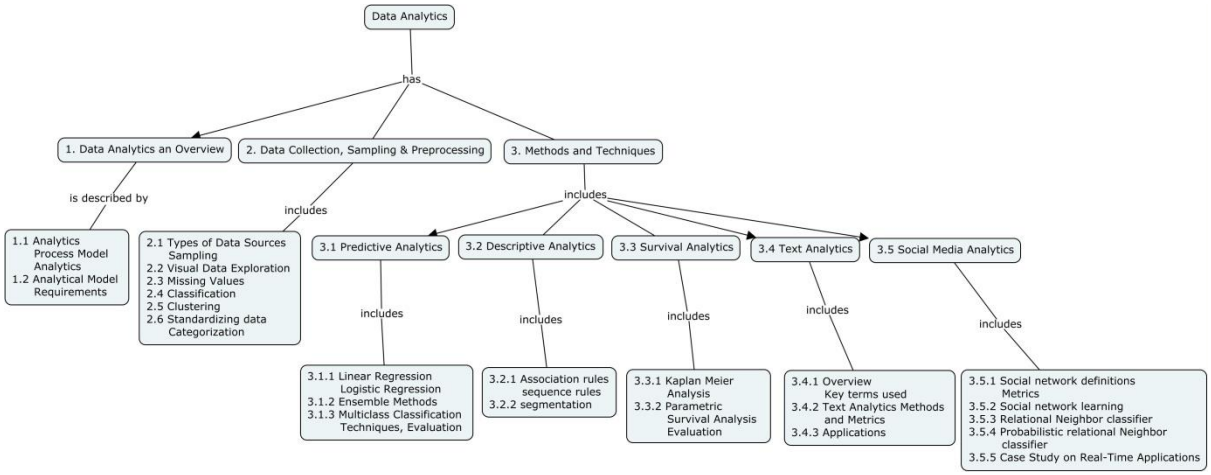
Course Outcome 3(CO3):

1. Prepare a predictive model for resource utilization by a computer system which has maximum size of RAM 512 MB, and 120 GB hard disk, which runs 6 processes at a given time with the time allotted for each of the process is about 2 milliseconds.
2. Point out the need for using a multiclass classification model in a system. Clearly provide the reasons over binary classification system with necessary illustrations
3. Depict a predictive model using multiclass classification techniques for any real-time application.

Course Outcome 4(CO4):

1. Interrogate the metrics and the methods in social network analytics for a bank ATM system with the standard for classifying the system into different sets of sub parts and justify with your proposed analytical model.
2. Consider an application of hospital management system which contains records of large set of patients in various diseases such as diabetes, heart disease, cancer. Apply the concept of ensemble methods to overcome the difficulties in maintaining the records in various departments in the hospital and also justify with the method that you have chosen for evaluation with the classification of the datasets across different disciplines.
3. Differentiate Kaplan Meier Analysis and parametric survival analysis.
4. Use ego nets and bigraphs for content management system.

Concept Map



Syllabus

Data Analytics an Overview– Analytics Process Model – Analytics – Analytical Model Requirements.

Data Collection, Sampling and Preprocessing – Types of Data Sources and Data Elements– Sampling – Visual Data Exploration – Missing Values –Classification-Clustering and Outlier detection – Standardizing data – Categorization.

Predictive Analytics – Linear Regression – Logistic Regression – Ensemble Methods – Multiclass Classification Techniques – Evaluating Predictive Models.

Descriptive Analytics – Association rules – sequence rules –segmentation.

Survival Analytics –Kaplan Meier Analysis –Parametric Survival Analysis – Evaluating Survival Analysis Models.

Text Analytics – Overview, key terms used – Text Analytics Methods – Text Analytics Metrics – Applications.

Social Network Analytics –Social network definitions – Social network metrics –Social network learning Relational Neighbor classifier -Probabilistic relational Neighbor classifier– Case Study on Real-Time Applications like Twitter data , dataset from Kaggle website, Data analytics for security applications and deep learning applications.

Reference Books

1. Bart Baesens, “Analytics in a Big Data World”, The Essential Guide to Data Science and its Applications, Wiley, First edition, 2014.
2. Jesus Rogel- Salazar, “Data Science and Analytics with Python “, CRC Press, First Edition, 2017.
3. Michael Berthold, David J. Hand, “Intelligent Data Analysis”, Springer, Second edition, 2007.
4. Thomas H. Davenport, Jeanne G. Harris, “Competing on Analytics: The New Science of Winning”, Harvard Business Review Press ,First edition,2007
5. Paul C. Zikopoulos, Chris Eaton, “Understanding Big Data”, McGraw-Hill, 2012 (eBook from IBM)
6. Chris Eaton, Dirk DeRoos, Tom Deutsch, George Lapis, Paul Zikopoulos, “Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data”, McGraw-Hill Publishing, 2012.

Websites

1. https://cognitiveclass.ai/courses/python-for-data-science

2. https://www.edx.org/course/introduction-to-r-for-data-science
3. https://www.edx.org/course/programming-for-data-science
4. https://www.coursera.org/learn/social-media-data-analytics
   https://www-935.ibm.com/services/us/gbs/thoughtleadership/chiefdataofficer/

Course Contents and Lecture Schedule

S.No.	Topic	No. of. Lectures
1.	**Data Analytics an Overview**	
1.1	Analytics Process Model, Analytics	1
1.2	Analytical Model Requirements	1
2	**Data Collection, Sampling and Pre-processing**	
2.1	Types of Data Sources and Data Elements, Sampling	1
2.2	Visual Data Exploration	1
2.3	Missing Values	1
2.4	Classification	1
2.5	Clustering and Outlier Detection	1
2.6	Standardizing data, Categorization	1
3	**Methods and Techniques**	
3.1	**Predictive Analytics**	
3.1.1	Linear Regression, Logistic Regression	2
3.1.2	Ensemble Methods	1
3.1.3	Multiclass Classification Techniques, Evaluation	1
3.2	**Descriptive Analytics**	
3.2.1	Association rules, Sequence Rules	1
3.2.2	Segmentation	1
3.3	**Survival Analytics**	
3.3.1	Kaplan Meier Analysis	1
3.3.2	Parametric Survival Analysis, Evaluation	1
3.4	**Text Analytics**	
3.4.1	Overview , Key Terms used	1
3.4.2	Text Analytics Methods and Metrics	1
3.4.3	Applications	1
3.5	**Social Network Analytics**	
3.5.1	Social network definitions , metrics	1
3.5.2	Social network learning	1
3.5.3	Relational Neighbor classifier	1
3.5.4	Probabilistic Relational Neighbor classifier	1
3.5.5	Case Study on Real-Time Applications like Twitter data, dataset from Kaggle website, security applications and deep learning applications.	1
Total Lectures		**24**

Lab Schedule

S. No	Name of Experiments	No. of. Sessions

1.	Study and installation of tools in data analytics such as Rapid miner, R, Python.	1
2.	Perform data pre-processing for the given dataset by performing data cleaning, data transformation, replacing the missing values and outlier data.	1
3.	Interprétation of the given data to perform Data clustering using Classical partitioning methods.	1
4.	Implémentation of Descriptive Analytics – Association rules – FP Growth - sequence rules.	1
5.	Implementation of Predictive analytics using linear and logistic regression for the given dataset	1
6.	Implementation of Predictive analytics using Decision trees.	1
7.	Implementation of Predictive analytics using Neural Network with Multi-class classification for the given dataset.	1
8.	Text analyticsusing NLP tools (SNLP/NLTK).	1
9.	Text analytics for applications like Fraud detection, Marketing, Scientific Applications, Web data clustering R/Python.	1
10.	Real time twitter data analytics using R.	1
11.	A Study on Data analytics for security methods and deep learning applications.	1
12.	Mini Project	1
Total Sessions		**12**

Course Designers:

Dr.C.Deisy cdcse@tce.edu
Mr.A.Sheik Abdullah asait@tce.edu
Dr.S.Sridevi sridevi@tce.edu

18IS270	ETHICAL HACKING AND CYBERFORENSICS LAB	Category	L	T	P	Credit
		PC	0	0	4	2

Preamble

The laboratory course on Ethical Hacking and Cyberforensics aims to provide hands on experience with hacking tools and techniques used by the information security professionals. Practical exposure on compliant and teaches the five phases of ethical hacking. The five phases include Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and Covering your Tracks.

Prerequisite

- Nil

Course Outcomes

On successful completion of the course, students will be able to

Course Outcomes		Bloom's Level	Expected Proficiency	Expected Level of Attainment (in %)
CO1	Utilize appropriate tools to apply footprinting, scanning network and enumeration techniques for the given scenario.	Apply	A	95
CO2	Analyze system vulnerabilities and harmful code embedded in application program or data.	Analyze	B	80
CO3	Perform penetration testing against Sniffing, Denial of service, Session Hijacking and SQL Injection attacks for the given scenario.	Analyze	B	80
CO4	Examine the given web server and web applications for detecting unpatched security flaws.	Analyze	B	80
CO5	Evade the given IDS and Firewall using appropriate tools.	Apply	A	95
CO6	Demonstrate various tools for evidence collection, acquisition from computer storage devices	Apply	A	95
CO7	Investigate the digital evidence using appropriate forensics tools.	Analyze	B	80

Mapping with ProgrammeOutcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	S	M	L		S			M	M	L	L
CO2	S	S	M		S			M	M	L	L
CO3	S	S	M		S			M	M	L	L
CO4	S	S	M		S			M	M	L	L
CO5	S	M	L		S			M	M	L	L
CO6	S	M	L		S			M	M	L	L
CO7	S	S	M		S			M	M	L	L

S - Strong, M – Medium, L – Low

Tools required

Kali Linux – Penetration Testing and Digital Forensics Linux Distribution
Url : https://tools.kali.org/tools-listing

Forensics Tools:
Tools like FTK Imager, The Sleuth kit (+Autospy), SANS SIFT and EnCase.

List of Experiments

Exp No.	Topic	No. of Lab Hours
1	Collect as much information as possible regarding a target network from publicly accessible sources.	4
2	Identify hosts, ports and services running in a network.	4
3	Extract usernames, machine names, network resources, shares and services from a system.	2
4	Test system and network for vulnerabilities and harmful plug-ins	4
5	Exploit and Test the target system with Malware	4
6	Sniff a network and analyze packets for attacks on the network.	2
7	Attack a computer or network that prevents legitimate use of its resources.	2
8	Exploit a valid computer session.	2
9	Demonstrate the hacking techniques of Web server.	4
10	Exploit vulnerabilities of Web Application to gain unauthorized access to a website or its associated data.	4
11	Perform SQL injection attack against non-validated input vulnerabilities of an web application.	2
12	Evade IDS and Firewall using appropriate hacking techniques.	2
13	Forensic evidence collection, checking and planning	4
14	Forensic evidence acquisition and backup	4
15	Forensic evidence Examination, deleted data recovery, reporting and evidence retention	4
	Total Lab Hours	**48**

Course Designers

1. C.Jeyamala jeyamala@tce.edu
2. M.Thangavel mtit@tce.edu

OUTCOME BASED EDUCATION

CURRICULUM AND DETAILED SYLLABI

FOR

M.E COMPUTER SCIENCE AND INFORMATION SECURITY DEGREE PROGRAMME

PROGRAMME ELECTIVES

FOR THE STUDENTS ADMITTED IN THE

ACADEMIC YEAR 2018-19 ONWARDS

THIAGARAJAR COLLEGE OF ENGINEERING

(A Government Aided ISO 9001:2008 certified Autonomous Institution affiliated to Anna University)

MADURAI – 625 015, TAMILNADU

Phone: 0452 – 2482240, 41
Fax: 0452 2483427
Web: www.tce.edu

LIST OF ELECTIVES

Course Code	Course Name
18ISPD0	Cloud Security
18ISPE0	IT Audit and Control
18ISPF0	Cyber Physical Systems
18ISPG0	Augmented Reality
18ISPH0	Artificial Intelligence

		Category	L	T	P	Credit
18ISPD0	**CLOUD SECURITY**	PC	3	0	0	3

Preamble

As organizations transition to cloud computing technology, security issues are a vital concern. In order to protect sensitive data and maintain regulatory compliance, the course must address the unique cyber security challenges faced when moving to a cloud environment. This course provides an experience of identifying and resolving the security issues specific to public and private clouds.

Prerequisite

- Nil

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcome		Blooms Level	Expected Proficiency	Expected level of attainment (%)
CO1:	Describe the design requirements of secure cloud architecture	Understand	A	85
CO2:	Utilize appropriate techniques to enable cloud data security for the given scenario.	Apply	B	75
CO3:	Adapt the security criteria's recommended to build the cloud infrastructure.	Apply	B	75
CO4:	Practice the secure software engineering principles for developing cloud applications.	Apply	B	75
CO5:	Examine the security concerns and operations involved in the cloud	Analyze	B	70

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1.	M	L									
CO2.	S	M	M		M	M			M		M
CO3.	S	M	M		M	M			M		M
CO4.	S	M	M		M	M			M		M
CO5.	S	S	M	L	M	M	M	M	M	M	M

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	Continuous Assessment Tests			Terminal Examination
	1	2	3	
Remember	20	20	20	20
Understand	40	20	20	20
Apply	40	50	40	40
Analyse	-	10	20	20
Evaluate	-	-	-	-
Create	-	-	-	-

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Explain cloud service models in detail.
2. What are the security concerns and risks associated with cloud architecture?
3. Summarize the cloud security architecture.

Course Outcome 2 (CO2):

1. Compare and contrast various storage architectures of cloud.
2. Apply security strategies for the given cloud architecture.
3. Explain digital rights management and policies.

Course Outcome 3 (CO3):

1. What are the security controls are applied to secure cloud platform.
2. Explain the disaster recovery and business continuity techniques to prevent data loss.
3. Interpret the security criteria for building internal cloud.

Course Outcome 4(CO4):

1. Discuss about the various cloud security apps.
2. Does authentication and authorization are needed for securing cloud applications.
3. Build secure cloud applications using secure software engineering principles.

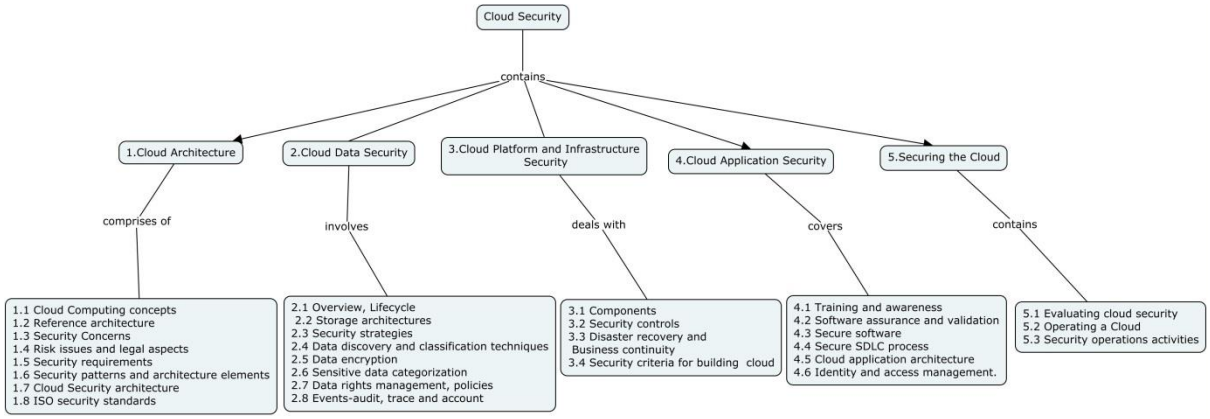
Course Outcome 5(CO5):

1. Explain the operations for securing cloud environment.
2. Illustrate the various security monitoring process involved in securing cloud.
3. Analyze the security concerns and operations of cloud environment.

Some of the Assignments topics are :(but not limited to)

1. Providing Cyber Security lab as a Service
2. Service deployment and usage over cloud
3. Managing cloud computing resources
4. Demonstrate existing cloud characteristics and service models
5. Performance evaluation of Services over cloud

Concept Map



Syllabus

Cloud Architecture: Cloud Computing concepts, Reference architecture, Security Concerns, Risk issues and legal aspects, Security requirements, Security patterns and architecture elements, Cloud Security architecture, ISO security standards.

Cloud Data Security: Overview, Lifecycle, Storage architectures, Security strategies, Data discovery and classification techniques, Data encryption: Application and limits, Sensitive data categorization, Data rights management, policies, Events-audit, trace and account.

Cloud Platform and Infrastructure Security: Components, Security controls, Disaster recovery and Business continuity, Security criteria for building an internal cloud and selecting an external cloud provider.

Cloud Application Security: Training and awareness, Software assurance and validation, Secure software, secure SDLC process, Cloud application architecture, Identity and access management.

Securing the cloud: Evaluating cloud security – checklist, metrics, security monitoring, best practices, Operating a Cloud – From architecture to secure operations, Security operations activities.

References

1. Daniel Carter, “CCSP Certified Cloud Security Professional All-in-One Exam Guide”, First edition, McGraw-Hill Education, 2017.
2. Vic (J.R.) Winkler, “Securing the Cloud: Cloud Computer Security Techniques and Tactics”, Syngress/Elsevier, First edition, 2011.
3. Brian T. O'Hara, Ben Malisow, “CCSP (ISC)2 Certified Cloud Security Professional Official Study Guide”, 1st edition, Wiley, 2017.
4. RajkumarBuyya, Christian Vecchiola, S.ThamaraiSelvi, “Mastering cloud computing”, Morgan Kaufman, 2013.
5. Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing”, 2011.
6. ObyVelte, Anthony Velte, Robert Elsenpeter, “Cloud Computing, A Practical Approach” McGraw-Hill Osborne Media; 1 edition [ISBN: 0071626948], 2009.

Course Contents and Lecture Schedule

Module No.	Topic	No. of Lecture Hours
1	**Cloud Architecture**	
1.1	Cloud Computing concepts	1
1.2	Reference architecture	1
1.3	Security Concerns	1
1.4	Risk issues and legal aspects	1
1.5	Security requirements	1
1.6	Security patterns and architecture elements	1
1.7	Cloud Security architecture	1
1.8	ISO security standards	1
2	**Cloud Data Security**	
2.1	Overview, Lifecycle	1
2.2	Storage architectures	1
2.3	Security strategies	2
2.4	Data discovery and classification techniques	1
2.5	Data encryption: Application and limits	1
2.6	Sensitive data categorization	2
2.7	Data rights management, Policies	2
2.8	Events-audit, trace and account	1
3	**Cloud Platform and Infrastructure Security**	
3.1	Components	1
3.2	Security controls	1
3.3	Disaster recovery and Business continuity	1
3.4	Security criteria for building an internal cloud and selecting an external cloud provider	2
4	**Cloud Application Security**	
4.1	Training and awareness	1
4.2	Software assurance and validation	1
4.3	Secure software	1
4.4	Secure SDLC process	1
4.5	Cloud application architecture	1
4.6	Identity and access management	1
5	**Securing the cloud**	
5.1	Evaluating cloud security	2
5.2	Operating a Cloud	2
5.3	Security operations activities.	2
	Total	**36**

Course Designers:

1. Dr.S.Padmavathi spmcse@tce.edu
2. Ms.C.Santhiya csit@tce.edu
3. Ms.J.John Shiny shinyit@tce.edu
4. Mr.M.Thangavel mtit@tce.edu

		Category	L	T	P	Credit
18ISPE0	**IT AUDIT AND CONTROL**	PE	3	0	0	3

Preamble

The course aims to provide an understanding of enterprise structure, policies, accountability mechanisms and monitoring practices in place to achieve the requirements of IT governance. Also, knowledge on security architecture (Policies, Standards, Procedures and Controls) and audit services in accordance with IT audit standards to ensure confidentiality, integrity and availability of information assets is provided.

Prerequisite

- Nil

Course Outcomes

On successful completion of the course, the students will be able to

Course Outcomes		**Bloom's Level**	**Expected Proficiency**	**Expected Level of Attainment (in %)**
CO1	Comprehend the basic concept of Auditing and Internal Controls	Understand	80	80
CO2	Recognize the information security policies, standards and procedures for completeness and alignment with generally accepted practices in IT Governance	Understand	80	80
CO3	Summarize the procedures and types for conducting Operating Systems audit	Apply	80	80
CO4	Solve the IT enterprise related issues in terms of confidentiality, integrity and availability of information.	Apply	80	80
CO5	Summarize the facts and concepts to be taken into account while conducting periodic reviews of information systems to determine whether they continue to meet the enterprise's objectives.	Apply	80	80
CO6	Compare the effectiveness of the IT governs structure to determine whether IT decisions, directions and performance support the enterprise's strategies and objectives.	Analyze	70	70
CO7	Apply Computer-Assisted Audit Tools and Techniques for testing Software, Networks	Apply	80	80

	and real time applications			

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1.	M	L	L									
CO2.	S	M					M		L	M		
CO3.	S	M	M		L		M		L	M		
CO4.	S	S	S		L		M			M		
CO5.	S	M			L		M			M		
CO6.	S	S	M						L	M		
CO7.	S	S	M		M		M		L			M

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	Continuous Assessment Tests			Terminal Examination
	1	2	3	
Remember	20	20	20	20
Understand	40	40	40	40
Apply	40	30	30	30
Analyze	-	10	10	10
Evaluate	-	-	-	-
Create	-	-	-	-

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. State the role of Audit Committee
2. State the authority of the Office of Internal Audit and the Purpose of Internal Audit report
3. List the responsible persons for internal controls and importance of IT Governance

Course Outcome 2 (CO2):

1. State the Procedure for selecting audits and examine the technique that management uses to addresses the IT issues.
2. Describe the Structure of the information technology function.
3. Identify the information security policies, standards and procedures for completeness

Course Outcome 3 (CO3):

1. Explain the audit procedures and control in different Operating systems- Windows/Linux/Mac/ Android
2. Report the issues identified in EDI
3. Identify the best audit procedures and practices for PC-based Accounting systems

Course Outcome 4 (CO4):

1. Experiment the Triggers of Data Integrity Loss through the following parameters
    a) Vulnerable code-in applications
    b) Unauthorized devices connected to the corporate network
    c) Inadequate or not applied segregation of duties (SoD)
    d) Inability to track the use of privileged passwords, particularly when passwords are shared
2. Report the Attacks on Data Integrity through Web site defacements, Logic bombs and Unauthorized modifications of operating systems etc, by the Following life cycle steps which includes
    a) Entering, creating and/or acquiring data
    b) Processing and/or deriving data
    c) Storing, replicating and distributing data
    d) Archiving and recalling data
    e) Backing up and restoring data
    f) Deleting, removing and destroying data
3. Relate the Standards and Best Practices for Risk Management and Compliance with the Security requirements for data management, information security with COBIT Deliver and Support and manipulate the improvement of the Data Integrity associated with it.

Course Outcome 5 (CO5):

1. Discuss the Disaster Recovery Plan Tests and Drill.
2. Describe how to Provide assurance that the processes for information systems operations, maintenance and support meet the organization's strategies and objectives
3. Predict the finest way of conducting periodic reviews of information systems.

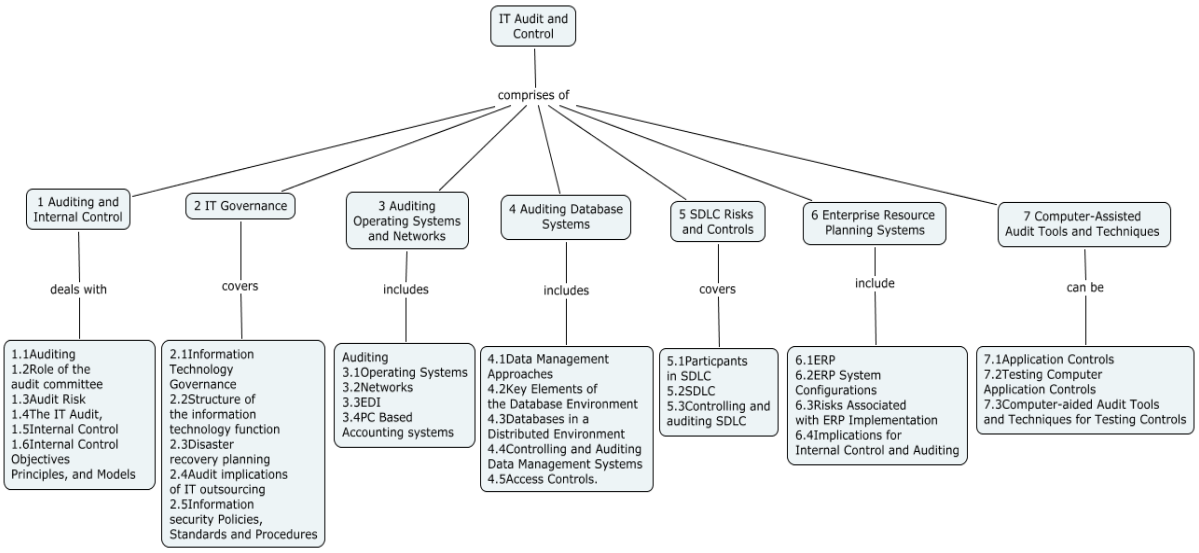
Course Outcome 6 (CO6):

1. Categorize the assurance for the necessary leadership and organization structure and point out the processes that are in place to achieve objectives and to support the organization's strategy.
2. Analyze the IT management and monitoring of controls (e.g., continuous monitoring, QA) for compliance with the organization's policies, standards and procedure.
3. Identify the actual problem and the incident management practices to determine whether incidents, problems or errors are recorded, analyzed and resolved in a timely manner.

Course Outcome 7 (CO7):

1. Compare different CAAT techniques for auditing Networks testing
2. Identify suitable computer assisted audit tools and techniques for software development life cycle in real time applications.
3. Analyze the CAATT for monitoring of application controls

Concept Map



Syllabus

Auditing and Internal Control: Overview of Auditing, Role of the audit committee ,Audit Risk ,The IT Audit, Internal Control, Internal Control Objectives, Principles, and Models.

IT Governance: Information Technology Governance, Structure of the information technology function, disaster recovery planning, audit implications of IT outsourcing.

Auditing Operating Systems and Networks: Auditing Operating Systems, Auditing Networks, Auditing Electronic Data Interchange (EDI),Auditing PC-Based Accounting Systems.

Auditing Database Systems: Data Management Approaches, Key Elements of the Database Environment, Databases in a Distributed Environment, Controlling and Auditing Data Management Systems, Access Controls.

SDLC risks and controls: Participants in Systems Development, the Systems Development Life Cycle, Controlling and Auditing the SDLC.

Enterprise Resource Planning Systems: ERP, ERP System Configurations, Risks Associated with ERP Implementation, Implications for Internal Control and Auditing.

Computer-Assisted Audit Tools and Techniques: Application Controls, Testing Computer Application Controls, Computer-aided Audit Tools and Techniques for Testing Controls.

References

1. James A. Hall, “Information Technology Auditing and Assurance”, South-Western cengage learning ,Third edition, 2011
2. Chris Davis and Mike Schiller, “IT Auditing: Using Controls to protect Information Assets”, Mc-Graw Hill, Second Edition, 2011
3. http://www.isaca.org/knowledge-center/itaf-is-assurance-audit-/IT-Audit-Basics/Pages/IT-Audit-Basics-Articles.aspx

4. http://intosaiitaudit.org/India_GeneralPrinciples.pdf
5. http://opentuition.com/wp-content/blogs.dir/1/files/group-documents/15/1289480671-COMPUTERASSISTEDAUDITTECHNIQUES.pdf

Course Contents and Lecture Schedule

Module No.	Topic	No. of Lectures
1	**Auditing and Internal Control**	
1.1	Overview of Auditing	1
1.2	Role of the audit committee	1
1.3	Audit Risk	1
1.4	The IT Audit	1
1.5	Internal Control	1
1.6	Internal Control Objectives, Principles, and Models.	2
2	**IT Governance**	
2.1	Information Technology Governance	1
2.2	Structure of the information technology function	2
2.3	Disaster recovery planning	1
2.4	Audit implications of IT outsourcing	1
2.5	Information security Policies, Standards and Procedures	1
3	**Auditing Operating Systems and Networks**	
3.1	Auditing Operating Systems	2
3.2	Auditing Networks	2
3.3	Auditing Electronic Data Interchange (EDI)	1
3.4	Auditing PC-Based Accounting Systems	2
4	**Auditing Database Systems**	
4.1	Data Management Approaches	1
4.2	Key Elements of the Database Environment	1
4.3	Databases in a Distributed Environment	1
4.4	Controlling and Auditing Data Management Systems	1
4.5	Access Controls	1
5	**SDLC risks and controls**	
5.1	Participants in Systems Development	1
5.2	The Systems Development Life Cycle	1
5.3	Controlling and Auditing the SDLC	1
6	**Enterprise Resource Planning Systems**	
6.1	ERP	1
6.2	ERP System Configurations	1
6.3	Risks Associated with ERP Implementation	1
6.4	Implications for Internal Control and Auditing	1
7	**Computer-Assisted Audit Tools and Techniques**	
7.1	Application Controls	1
7.2	Testing Computer Application Controls	1
7.3	Computer-aided Audit Tools and Techniques for Testing Controls	2
	Total Lectures	**36**

Course Designers:

1. R.Suganya rsuganya@tce.edu
2. E.Ramanujam erit@tce.edu

18ISPF0	Cyber Physical Systems	Category	L	T	P	Credit
		PE	3	0	0	3

Preamble

The course aims to provide an understanding of the principles of Cyber Physical System, Platform and components for CPS and modeling techniques of CPS. It also includes security of CPS with basic and advanced techniques. This course ends with the module of various CPS application case-studies.

Prerequisite

NIL

Course Outcomes

On successful completion of the course, students will be able to

Course Outcomes		Bloom's Level	Expected Proficiency	Expected Level of Attainment (in %)
CO1	Explain the principles of Cyber Physical Systems (CPS) with Industry 4.0 and building automation.	Understand	A	85
CO2	Identify the platform components in both hardware and software for supporting CPS	Understand	A	80
CO3	Apply the suitable CPS modeling techniques for the given problem	Apply	B	80
CO4	Illustrate the various security techniques and attacks in CPS	Apply	B	75
CO5	Examine the given scenario to implement a CPS with the reference of the case-study problems such as Medical CPS, Agriculture CPS etc	Analyze	B	70

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	M	L									L
CO2	M	L									L
CO3	S	M	L		M						L
CO4	M	M	L		L						L
CO5	S	S	M	L	M	M	M	M	M		M

S - Strong, M – Medium, L – Low

Assessment Pattern

Bloom's Assessment Category	CAT 1	CAT 2	CAT 3	Terminal Exam
Remember	20	20	20	20
Understand	40	30	30	30
Apply	40	50	50	50
Analyze	-	-	-	-
Evaluate	-	-	-	-
Create	-	-	-	-

CO5 is attained only through case-study

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Discuss the Evolution of Industry 4.0

2. Provide representative circuit diagram of a Successive approximation based Analog to Digital Converter and explain its working principle.

3. Describe the architecture of IIoT.

Course Outcome 2 (CO2):

1. Explain three key differences between RISC and CISC processors.

2. In a two-level cache system, the access times of L1 and L2 caches are 1 and 8 clock cycles respectively. The miss penalty from L2 cache to main memory is 18 clock cycles. The miss rate of L1 cache is twice that of L2. The average memory access time of the cache system is 2 cycles.
   Compute the L1 and L2 cache miss rates.

3. Consider a set of two tasks and show that if they are schedulable with any fixed priority scheduling algorithm then they are also schedulable with RM Scheduling.

Course Outcome 3 (CO3):

1. Describe with example the formal tuple of a Timed Automaton. Define the two different types of transitions in a Timed Automaton.

2. Construct a Timed Automaton which satisfies the following specification. The automata accepts an infinite sequence of events abababababab... if the following timing constraints are satisfied.
   i. The i-th b is accepted only if it arrives at time t = i,

ii. Let the i-th a come at Ti, the i-th b come at Ti', the (i + 1)-th a come at Ti+1 and the (i+1)-th b come at T'i+1. It is always the case that T'_{i+1} - Ti+1 < T 'i -Ti for the input events to be accepted.

Note that a Timed Automaton only contains clock constraints and invariants of the form c <= k or c >=k for c being a clock and k being any numerical constant.

3. Consider the following program

   x Ɛ [0; 10]
   while(x<=9)
   x=x+3;
   Demonstrate how interval/range analysis can be performed on the above program for revealing the possible value ranges for x at each program point at the end of execution. Elaborate the method starting with construction of the control flow graph (CFG) and the set of data flow equations.

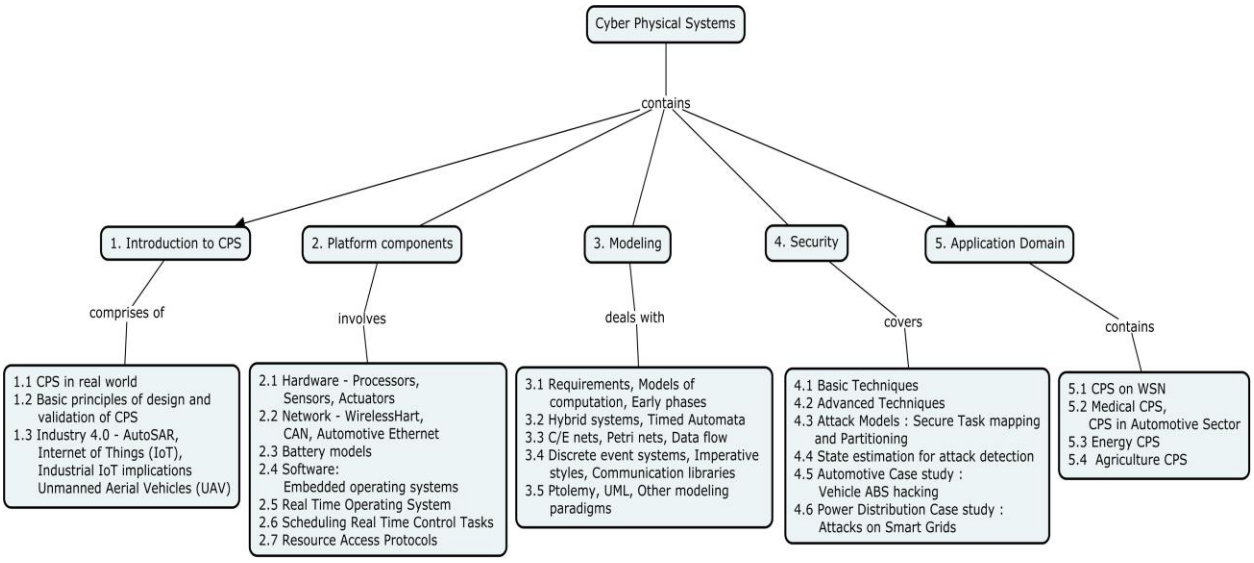
Course Outcome 4 (CO4):

1. Draw the control theoretic model of a Cyber Physical System considering that an attacker can spoof the data sensed from plant output. Explain with suitable formulation how a threshold based detector system can detect such attacks.

2. What are replay attacks, why are they considered convenient (from an attacker's point of view) in the context of feedback control systems?

3. Apply the principles of State estimation for attack detection in a cyber physical systems which is subject to switching signal attacks and injection of counterfeit measurements.

Concept Map



Syllabus

Introduction to cyber physical Systems (CPS): CPS in real world - Basic principles of design and validation of CPS - Industry 4.0 - AutoSAR, Internet of Things (IoT), Industrial IoT implications - Unmanned Aerial Vehicles (UAV).

Platform components: Hardware - Processors, Sensors, Actuators - Network - WirelessHart, CAN, Automotive Ethernet - Battery models. Software: Embedded operating systems - Real Time Operating System - Scheduling Real Time Control Tasks - Resource Access Protocols.

Modeling: Requirements, Models of computation, Early phases, Hybrid systems, Timed Automata, C/E nets, Petri nets, Data flow, Discrete event systems, Imperative styles, Communication libraries, Ptolemy, UML, Other modeling paradigms.

Security: Basic Techniques, Advanced Techniques, Attack Models : Secure Task mapping and Partitioning - State estimation for attack detection - Automotive Case study : Vehicle ABS hacking - Power Distribution Case study : Attacks on Smart Grids.

Application Domain: CPS on WSN, Medical CPS, CPS in Automotive sector, Energy CPS and Agriculture CPS.

References

1. E. A. Lee, Sanjit Arunkumar Seshia, "Introduction to Embedded Systems – A Cyber–Physical Systems Approach" , MIT Press, Second Edition, 2017.
2. Rajeev Alur “Principles of Cyber-Physical Systems” , The MIT Press, 2015.
3. Peter Marwedel, "Embedded Systems Design - Embedded Systems Foundations of cyber Physical Systems and the Internet of things, Springer, Third Edition, 2018.
4. Raj Rajkumar, Dionisio, klein, Cyber Physical Systems, Pearson Education , 2017
5. https://ptolemy.berkeley.edu/projects/chess/
6. https://ptolemy.berkeley.edu/projects/cps/
7. https://www.coursera.org/learn/cyber-physical-systems-1

Course Contents and Lecture Schedule

Module No	Topic	No. of Lecture Hours
1	**Introduction to cyber physical Systems(CPS)**	
1.1	CPS in real world	1
1.2	Basic principles of design and validation of CPS	1
1.3	Industry 4.0 - AutoSAR, Internet of Things (IoT), Industrial IoT implications - Unmanned Aerial Vehicles(UAV)	2
2	**Platform components**	
2.1	Hardware - Processors, Sensors, Actuators	1
2.2	Network - WirelessHart, CAN, Automotive Ethernet	1
2.3	Battery models	1
2.4	Software: Embedded operating systems	1
2.5	Real Time Operating System	2
2.6	Scheduling Real Time Control Tasks	1
2.7	Resource Access Protocols	1
3	**Modeling**	
3.1	Requirements, Models of computation, Early phases	1
3.2	Hybrid systems, Timed automata	1
3.3	C/E nets, Petri nets and data flow	2
3.4	Discrete event systems, Imperative styles, Communication libraries	1
3.5	Ptolemy, UML, other modeling paradigms	2
4	**Security**	
4.1	Basic Techniques	1
4.2	Advanced Techniques	2
4.3	Attack Models : Secure Task mapping and Partitioning	2
4.4	State estimation for attack detection	1
4.5	Automotive Case study : Vehicle ABS hacking	2
4.6	Power Distribution Case study : Attacks on Smart Grids	2
5.	**Application Domain**	
5.1	CPS on WSN	2
5.2	Medical CPS, CPS in Automotive sector	2
5.3	Energy CPS	1
5.4	Agriculture CPS	2
	Total Hours	36

Course Designers

1. Dr. P.Karthikeyan karthikit@tce.edu
2. Mr. M.Manikandakumar mmrit@tce.edu

		Category	L	T	P	Credit
18ISPGO	**AUGMENTED REALITY**	PC	3	0	0	3

Preamble

This course emphasizes on augmented reality systems, tracking technologies and interactions between the real and virtual environments. It also focuses on collaborative augmented reality and mobile augmented reality.

Prerequisite

- Nil

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcome		Blooms Level	Expected Proficiency	Expected level of attainment (%)
CO1:	Observe the working principle of AR and able to differentiate Virtual Reality, Augmented Reality and Mixed Reality	Understand	B	85
CO2:	Summarize the characteristics of tracking system and principles behind the interaction.	Understand	B	85
CO3:	Interpret interactions required for tracking any augmented reality applications	Apply	B	85
CO4:	Use collaborative interfaces to develop new 3D augmented reality applications	Apply	B	80
CO5:	Investigate the tracking methodology and interfaces used in real time applications.	Analyze	B	70
CO6:	Develop mobile augmented reality application for any of the real time scenario	Create	B	70

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1.	**L**	**L**							**L**		
CO2.	**L**	**L**							**L**	**L**	
CO3.	**M**	**L**	**L**		**S**			**M**	**M**	**M**	
CO4.	**M**	**L**	**L**		**S**			**M**	**M**	**M**	
CO5.	**M**	**M**	**M**	**L**	**S**	**L**		**L**	**M**	**M**	
CO6.	**M**	**S**	**S**		**S**	**M**	**L**	**M**	**S**	**S**	

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	Continuous			Terminal Examination
	1	2	3	
Remember	0	0	0	0
Understand	40	30	30	30
Apply	60	30	40	40
Analyse	0	20	30	30
Evaluate	0	0	0	0
Create	0	0	0	0

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Define Augmented Reality.
2. Differentiate virtual reality, augmented reality and mixed reality.
3. State Milgram–Weiser chart

Course Outcome 2 (CO2):

1. List various coordinate systems that supports tracking.
2. Describe all the characteristics of tracking terminologies.
3. How targets are matched using spherical markers.

Course Outcome 3 (CO3):

1. Illustrate the working principle of natural feature tracking and identify the scenes that match the given marker.
2. Describe in detail the simultaneous localization and mapping algorithm for path planning in exploring your city.
3. Use mobile sensors to illustrate the optical tracking system.

Course Outcome 4 (CO4):

1. Explain in detail the interfaces that are mandate for AR collaboration.
2. Design a 3D multimodal AR application with Graphical user Interface.
3. Illustrate the working principle of Outdoor tracking.

Course Outcome 5 (CO5):

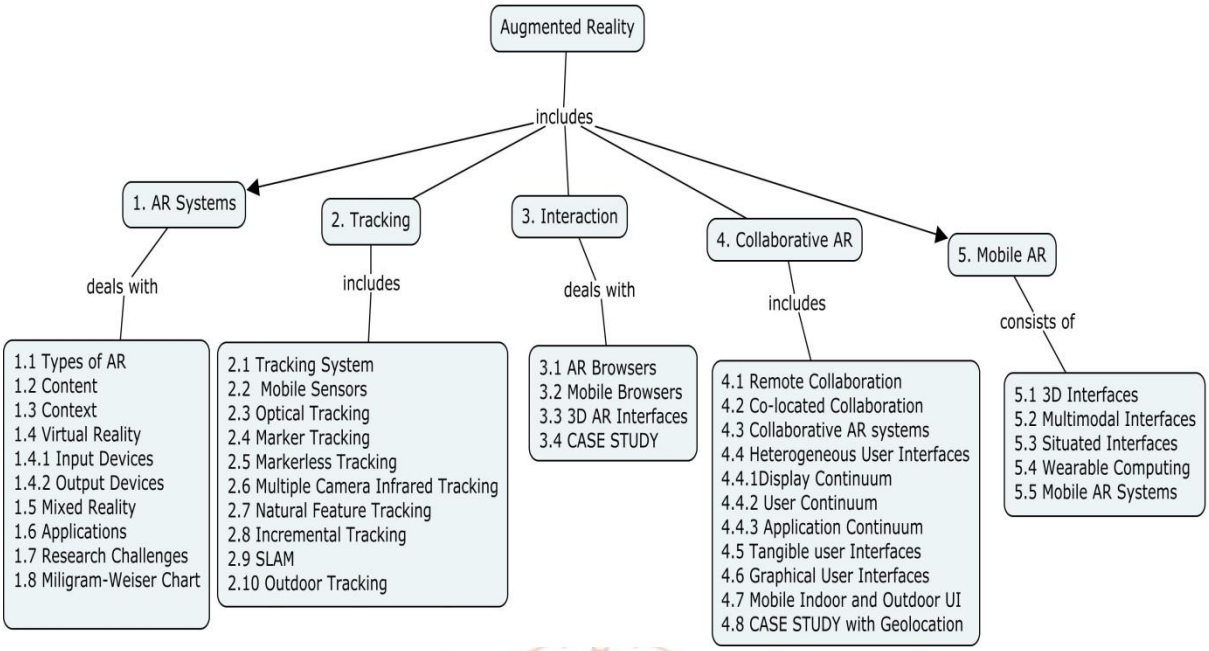
1. Discriminate marker tracking and markerless tracking and apply suitable tracking technique in robot path planning.
2. Construct an AR application using Web 2.0 that imitates an IoT application using ARIoT kit.
3. Discriminate the principle of video conferencing and check how it matches with holographic projection.

Course Outcome 6 (CO6):

This CO is purely assessed with assignments. The assignment is a AR product development. The products can be [but not limited to]

- AR Books
- AR Menu cards
- AR Cinema
- AR Game
- AR Search Engine

Concept Map



Syllabus

Augmented Reality(AR): Types of AR – Content – Context - Virtual Reality – Types – Input Devices – Output Devices – Mixed Reality Continuum – Applications – Research Challenges - Milgram–Weiser chart.

Tracking : Characteristics - Tracking systems – Mobile sensors - Optical Tracking – Marker tracking – Markerless Tracking - Multiple Camera Infrared tracking – Natural Feature Tracking – Incremental Tracking – Simultaneous Localization and Mapping – Outdoor Tracking – Case study on Augmenting Your City Map

Interaction: AR browsers – Mobile AR browsers such as Aurasma, Junaio, Mixare etc.- 3D AR interfaces; Tangible interfaces and augmented interfaces – Case study on Augmented Book

Collaborative Augmented Reality: Remote Collaboration- Video conferencing- Co-located Collaboration; Collaborative AR systems - Heterogeneous user interfaces: Display Continuum, User Continuum, Application Continuum; Tangible User Interfaces, Graphical User Interfaces, Mobile Indoor and Outdoor UI- Case study on Augmented Reality with Geolocation

Mobile Augmented Reality: 3D, Multimodal, Situated Interfaces- Wearable computing – Mobile AR systems – Customizing an augmented reality game.

Reference Books

- Dieter Schmalstieg, Tobias HollereR, "Augmented Reality: Principles and Practice, Pearson education, 2016.
- Gregory C. Burdea & Philippe Coiffet , “Virtual Reality Technology”, Second Edition, John Wiley & Sons, Inc., © 2003-2017.

Websites

- Augmented Reality and Video streaming Services - https://www.coursera.org/learn/ar-technologies-video-streaming?authMode=login
- Getting started with augmented reality - https://www.coursera.org/learn/augmented-reality?
- Introduction to Augmented reality and AR Core - https://www.coursera.org/learn/ar?
- A Beginner's Guide to Augmented Reality with Unity - https://www.udemy.com/augmented_reality_with_unity/
- Build 12 Augmented Reality (AR) apps with Unity & Vuforia - https://www.udemy.com/develop-augmented-reality-book-ar-business-card-with-unity/

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1.	**Augmented Reality(AR)**	
1.1	Types of AR	1
1.2	Content	1
1.3	Context	
1.4	Virtual Reality(VR)	1
1.4.1	Types of VR	
1.4.2	Input Devices	1
1.4.3	Output Devices	
1.5	Mixed Reality Continuum	1
1.6	Applications	
1.7	Research Challenges	1
1.8	Milgram–Weiser chart	
2.	**Tracking**	
2.1	Tracking systems	1
2.2	Mobile sensors	1
2.3	Optical Tracking	1
2.4	Marker tracking	1
2.5	Markerless Tracking	1
2.6	Multiple Camera Infrared tracking	1
2.7	Natural Feature Tracking	1
2.8	Incremental Tracking	1
2.9	Simultaneous Localization and Mapping	1
2.10	Outdoor Tracking	1
2.11	Case study on Augmenting Your City Map	2
3.	**Interaction**	
3.1	AR browsers	1
3.2	Mobile AR browsers	1
3.3	3D AR interfaces	1
3.3.1	Tangible interfaces	1
3.3.2	Augmented interfaces	
3.4	Case study on Augmented Book	1
4.	**Collaborative Augmented Reality**	
4.1	Remote Collaboration- Video conferencing	2
4.2	Co-located Collaboration	1

S.No.	Topic	No. of Lectures
4.3	Collaborative AR systems	1
4.4	Heterogeneous user interfaces	1
4.4.1	Display Continuum	1
4.4.2	User Continuum	
4.4.3	Application Continuum	
4.5	Tangible Interfaces	1
4.6	Graphical User Interfaces	
4.7	Mobile Indoor and Outdoor UI	1
4.8	Case study on Augmented Reality with Geolocation	1
5.	**Mobile Augmented Reality**	
5.1	3D, Multimodal, Situated Interfaces	1
5.2	Wearable computing	1
5.3	Mobile AR systems	1
5.4	Case Study: Customizing an augmented reality game	1
Total Lectures		**36**

Course Designers:

1. Dr.S.Muthuramalingam smrit@tce.edu
2. Ms. T.Manju tmanju@tce.edu

18ISPH0	ARTIFICIAL INTELLIGENCE	Category	L	T	P	Credit
		PE	3	0	0	3

Preamble

The objective of the course is to make the students to learn the basic concepts intelligent agents and games. Knowledge Representation, uncertain knowledge and reasoning makes the student to approach the uncertainty problems in real world. Advance concept like reinforcement learning and agent based modeling with case studies will experience them to explore the real world problems.

Prerequisite

NA

Course Outcomes

On the successful completion of the course, students will be able to

CO	Course Outcome	Bloom's Level
CO1	Comprehend the basic concepts and techniques of intelligent agents	Understand
CO2	Construct adversarial problems and approaches to game design	Apply
CO3	Construct knowledge representation, uncertain knowledge and reasoning	Apply
CO4	Compare the uncertainty with respect to different parameters and find the reasoning to approach the uncertainty	Analyze
CO5	Develop a RL algorithms in active and dynamic levels for Elevator control system	Apply
CO6	Implement Simple Decision problems (Airport Sitting Problem), Complex Decision (Game Theory)	Apply
CO7	Construct Agent Based Modelling to farming behaviour	Apply

Mapping with Programme Outcomes

Cos	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	L	M	M								
CO2	M	L	L		S			M	M	M	
CO3	M	L	L		S			M	M	M	
CO4	M	L	L		S		L	M	M	M	M
CO5	M	L	L		S		L	M	M	M	
CO6	M	L	L		S	L	L	M	M	M	
CO7	M	L	L		S		L	M	M	M	

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	Continuous Assessment Tests			Terminal Examination
	1	2	3	
Remember	0	0	0	0
Understand	60	30	20	20
Apply	30	50	40	40
Analyse	10	20	40	40
Evaluate	0	0	0	0
Create	0	0	0	0

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. List the feature of Utility agent
2. What are planning graphs? Explain the methods of planning and acting in the real world.
3. How adversarial search differ from heuristic

Course Outcome 2 (CO2):

1. How heuristic values are calculated for OLA application for route finding
2. How for Inclusion of element as a choice is helpful for game designer point of view
3. List the features of partial order planning

Course Outcome 3 (CO3):

1. State ridges role in local optimization problems
2. List the components of optimal game designing
3. Write the formula for Q Learning

Course Outcome 4 (CO4):

1. Illustrate how partial order planning applied for flat tyre problem.
2. Illustrate the agent based modelling features for traffic problem.

Course Outcome 5 (CO5):

1. Explain how Non-deterministic rewards and actions are obtained in Q-learning.
2. Illustrate how decision network representation was done for airport sitting problem.

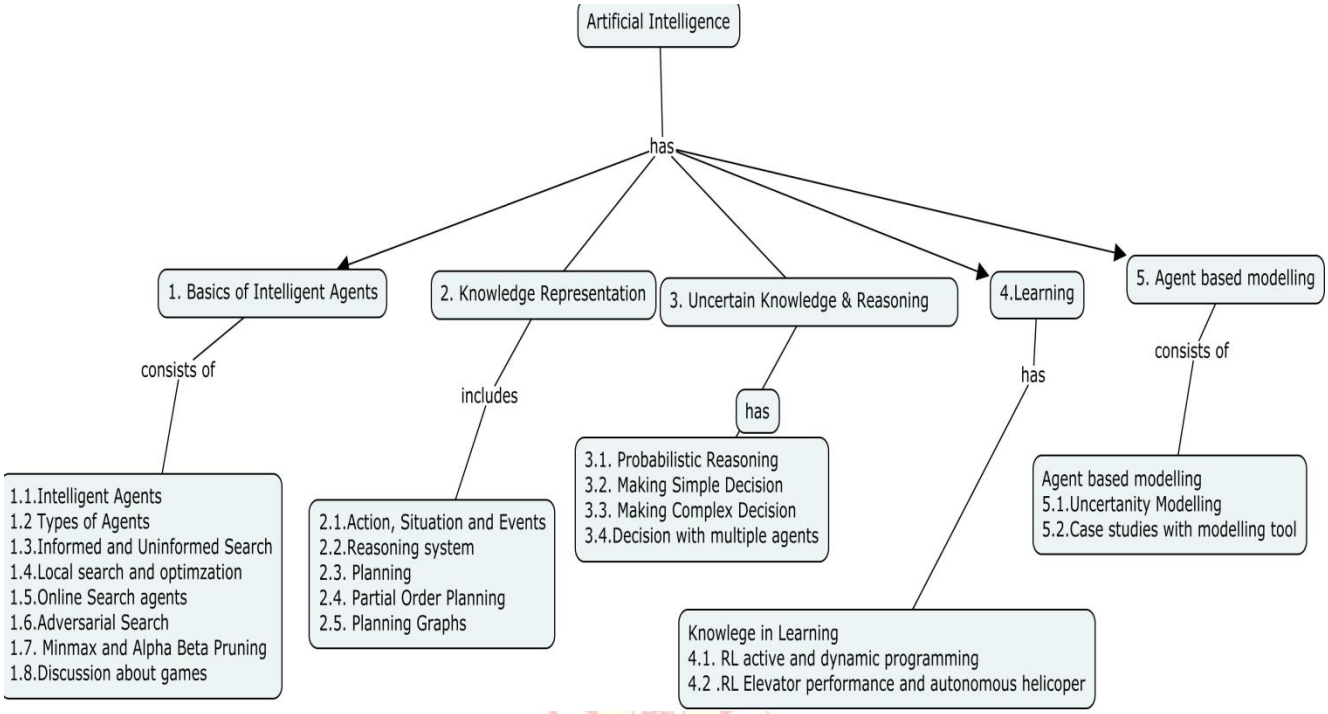
Course Outcome 6 (CO6):

1. List and relate how reinforcement learning algorithm for unmanned helicopter is used for taking decision
2. List the ways to model an agent based human behaviour with heuristic algorithm.

Course Outcome 7 (CO7):

1. Apply the RL technique for the 4 elevators in a ten story building. if passengers on several floors have requested pickups, which should be served first? If there are no pickup requests, how should the elevators distribute themselves to await the next request? Apply the reinforcement learning for finding the optimal strategy for the elevator to satisfy the commercial dispatching needs of people waiting to be less.
2. Apply agent based modelling for the city traffic and the modelling features to support for uncertainty in the traffic
3. Apply Mobile robot path planning using partial order planning

Concept Map



Syllabus

Basics of Intelligent Agents – Comparison of Informed and Uninformed Search – Adversarial Search – Games – Game Theory - Discussion about games (Contextual, Technical, Socio-cultural, Player, Multiagent)

Knowledge Representation – Action, situation and events – Mental events and objects – Planning Problems – Partial Order Planning – Planning Graphs – Mobile Robot Path Planning

Uncertain Knowledge and Reasoning – Quantifying Uncertainty – Probabilistic Reasoning – Probabilistic Reasoning over time – Making Simple decision – Making complex decision.

Learning –Knowledge in Learning – Logical formulation of learning – Reinforcement Learning – Active and Dynamic Reinforcement Learning – Case Studies about elevator performance improvement , Autonomous helicopter planning

Agent Based Modelling – Features of agent based modelling - Uncertainty Modelling – Auction Theory - Real World problems modelling using Netlogo tool for Boids simulation, Farming Behaviour

Reference Books

1. Stuart Russell and Peter Norvig., "Artificial Intelligence: A Modern Approach", Pearson, third edition, 2017.
2. Elaine Rich., Kevin Knight and Shivashankar B. Nair., **"**Artificial Intelligence", McGraw-Hill Education; 3rd edition, 2009.

Websites

1. http://ccl.northwestern.edu/netlogo/
2. https://sites.google.com/site/matteorichiardi/jas-mine
3. https://sites.google.com/site/matteorichiardi/teaching/abm-oxford

Course Contents and Lecture Schedule

Module No.	Topic	No. of Lectures
1	**Introduction**	1
1.1	Agents and Environment, Intelligent Agent	2
1.2	Types of Agents with examples	1
1.3	Informed and Uninformed Search	1
1.4	Local search and optimization problems	1
1.5	Online search agents and unknown environments	1
1.6	Adversarial search	1
1.7	Minmax Algorithm and Alpha Beta pruning	1
1.8	Game theory	2
1.8	Discussion about games (Contextual, Technical, Socio-cultural, Player, Multiagent)	1
2	**Knowledge Representation**	1
2.1	Action, situation and events – Mental events and objects	1
2.2	Reasoning systems for categories	1
2.3	Planning introduction	1
2.4	Partial Order Planning	1
2.5	Planning Graphs, Mobile Robot Path Planning	2
3	**Uncertain Knowledge and Reasoning**	2
3.1	Probabilistic Reasoning – Probabilistic Reasoning over time	1
3.2	Making Simple decision – Utility function	2
3.3	Making complex decision – sequential decision problems	1
3.4	Decision with multiple agents – Game Theory	2
4	**Learning –Knowledge in Learning**	1
4.1	Reinforcement Learning – Active and Dynamic programming	2
4.2	Reinforcement Learning – Elevator Performance and Autonomous Helicopter	1
5	**Agent Based Modelling – features**	1
5.1	Uncertainty Modelling	1
5.2	Auction Theory	2
5.1	Case Studies with Modelling Tool (Net Logo) – Boids Simulation and Farming Behaviour	1
	Total Lectures	**36**

Course Designers:

1. Dr.D.Tamilselvi dtamilselvi@tce.edu
2. Ms.T.Manju tmanju@tce.edu

18PGAA0	PROFESSIONAL AUTHORING

Category	L	T	P	Credit
AC	2	0	0	2

Preamble

On the successful completion of the course, the students will be able to:

1. Explain how to improve your writing skills and level of readability
2. Write each section of research paper
3. Write good quality technical paper

Syllabus

Planning and Preparation, Word Order, Breaking up long sentences, Structuring Paragraphs and Sentences, Being Concise and Removing Redundancy, Avoiding Ambiguity and Vagueness

Clarifying Who Did What, Highlighting Your Findings, Hedging and Criticising, Paraphrasing and Plagiarism, Sections of a Paper, Abstracts. Introduction

Review of the Literature, Methods, Results, Discussion, Conclusions, The Final Check.

Key skills for writing a Title, writing an Abstract, writing an Introduction, writing a Review of the Literature,

Skills for Writing the Methods, Results, Discussion and Conclusions
Useful phrases, how to ensure paper is as good as it could possibly be the first- time submission

Assessment Pattern

Abstract	:	10
Introduction	:	10
Literature Review	:	10
Research Question	:	10
Methods	:	10
Results and Discussion	:	10
Conclusions	:	10
Appropriateness of Title	:	05
Quality of the Paper and Plagiarism	:	25

References

1. Goldbort R, 'Writing for Science', Yale University Press, 2006
2. Day R, 'How to Write and Publish a Scientific Paper', Cambridge University Press, 2006
3. Highman N, 'Handbook of Writing for the Mathematical Sciences, SIAM Highman's book, 1998
4. Adrian Wallwork, 'English for Writing Research Papers', Springer New York Dordrecht Heidelberg London, 2011

18PGAB0	VALUE EDUCATION

Category	L	T	P	Credit
AC	2	0	0	2

Preamble

On the successful completion of the course, the students will be able to:

1. Experience self-development
2. Explain the importance of Human values
3. Develop the overall personality

Syllabus

Values and self-development –Social values and individual attitudes. Work ethics, Indian vision of humanism. Moral and non- moral valuation. Standards and principles, Value judgements

Importance of cultivation of values, Sense of duty. Devotion, Self-reliance. Confidence, Concentration. Truthfulness, Cleanliness, Honesty, Humanity, Power of faith, National Unity, Patriotism, Love for nature, Discipline

Personality and Behavior Development, Soul and Scientific attitude, Positive Thinking. Integrity and discipline, Punctuality, Love and Kindness, Avoid fault Thinking, Free from anger, Dignity of labour, Universal brotherhood and religious tolerance, True friendship, Happiness Vs suffering, love for truth.

Aware of self-destructive habits, Association and Cooperation, Doing best for saving nature

Character and Competence –Holy books vs Blind faith, Self-management and Good health, Science of reincarnation, Equality, Nonviolence , Humility, Role of Women, All religions and same message, Mind your Mind, Self-control, Honesty, Studying effectively

Assessment Pattern

Bloom's Category	Continuous Assessment Test	Terminal Examination
Remember	20	20
Understand	40	40
Apply	40	40
Analyse	0	0
Evaluate	0	0
Create	0	0

References

1. Chakroborty, S.K. "Values and Ethics for organizations Theory and practice", OxforUniversity Press, New Delhi

OUTCOME BASED EDUCATION

CURRICULUM AND DETAILED SYLLABI

FOR

M.E COMPUTER SCIENCE AND INFORMATION SECURITY DEGREE PROGRAMME

PROGRAMME CORE

FOR THE STUDENTS ADMITTED IN THE

ACADEMIC YEAR 2018-19 ONWARDS

THIAGARAJAR COLLEGE OF ENGINEERING

(A Government Aided ISO 9001:2008 certified Autonomous Institution affiliated to Anna University)

MADURAI – 625 015, TAMILNADU

Phone: 0452 – 2482240, 41
Fax: 0452 2483427
Web: www.tce.edu

THIAGARAJAR COLLEGE OF ENGINEERING: MADURAI – 625 015
M.E Degree (Computer Science and Information Security) Program
COURSES OF STUDY
(For the candidates admitted from 2018-2019 onwards)

THIRD SEMESTER

Subject code	Name of the Course	Category	No. of Hours / Week			credits
			L	T	P	
THEORY						
14ISPX0	Elective-IV	PE	3	-	-	3
OPEN ELECTIVE						
18ISGA0	Data Analytics	OE	2	-	-	2
PRACTICAL						
18IS380	Dissertation Phase I	PC	-	-	20	10
Total			**5**	**-**	**20**	**15**

PC : Program Core
PE : Program Elective
CC : Common Core
AC : Audit Course
OE : Open Elective

L : Lecture
T : Tutorial
P : Practical

Note:

1 Hour Lecture is equivalent to 1 credit
2 Hours Tutorial is equivalent to 1 credit
2 Hours Practical is equivalent to 1 credit

THIAGARAJAR COLLEGE OF ENGINEERING: MADURAI – 625 015

M.E Degree (Computer Science and Information Security) Program

SCHEME OF EXAMINATIONS

(For the candidates admitted from 2014-2015 onwards)

THIRD SEMESTER

S.No.	Sub. code	Name of the Course	Duration of Terminal Exam. in Hrs.	Marks			Minimum Marks for Pass	
				Continuous Assessment *	Terminal Exam **	Max. Marks	Terminal Exam	Total
THEORY								
1	14ISPX0	Elective-IV	3	50	50	100	25	50
OPEN ELECTIVE								
2	18ISGA0	Data Analytics	3	50	50	100	25	50
PRACTICAL								
3	18IS380	Dissertation Phase I	-	150	150	300	75	150

* Continuous Assessment evaluation pattern will differ from subject to subject and for different tests. This will have to be declared in advance to students. The department will put a process in place to ensure that the actual test paper follow the declared pattern.

** Terminal Examination will be conducted for maximum marks of 100 and subsequently be reduced to 50 marks for the award of terminal examination marks.

THIAGARAJAR COLLEGE OF ENGINEERING: MADURAI – 625 015
M.E Degree (Computer Science and Information Security) Program
COURSES OF STUDY
(For the candidates admitted from 2018-2019 onwards)

FOURTH SEMESTER

Subject code	Name of the Course	Category	No. of Hours / Week			credits
			L	T	P	
PRACTICAL						
18IS480	Dissertation Phase II	PC	-	-	15	15
Total			**-**	**-**	**15**	**15**

PC : Program Core
PE : Program Elective
CC : Common Core
AC : Audit Course
OE : Open Elective

L : Lecture
T : Tutorial
P : Practical

Note:

1 Hour Lecture is equivalent to 1 credit
2 Hours Tutorial is equivalent to 1 credit
2 Hours Practical is equivalent to 1 credit

THIAGARAJAR COLLEGE OF ENGINEERING: MADURAI – 625 015

M.E Degree (Computer Science and Information Security) Program

SCHEME OF EXAMINATIONS

(For the candidates admitted from 2018-2019 onwards)

FOURTH SEMESTER

S.No.	Sub. code	Name of the Course	Duration of Terminal Exam. in Hrs.	Marks			Minimum Marks for Pass	
				Continuous Assessment *	Terminal Exam **	Max. Marks	Terminal Exam	Total
PRACTICAL								
1	18IS480	Dissertation Phase II	-	150	150	300	75	150

* Continuous Assessment evaluation pattern will differ from subject to subject and for different tests. This will have to be declared in advance to students. The department will put a process in place to ensure that the actual test paper follow the declared pattern.

** Terminal Examination will be conducted for maximum marks of 100 and subsequently be reduced to 50 marks for the award of terminal examination marks.

18ISGA0	DATA ANALYTIC TECHNIQUES	Category	L	T	P	Credit
		OE	2	0	0	2

Preamble

The course on Data Analytics aims to emphasize the in depth coverage focusing different analytic techniques structured around broad contour of Predictive, Descriptive, Text, and Survival Analytics. This course targets at facilitating the students to understand the various functionalities of Data Analytics and perform many operations related to creating, using and maintaining databases for Real-world applications and emerging technologies in Data Analytics.

Prerequisite

- **Nil**

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcome		Blooms Level	Expected Proficiency	Expected level of attainment (%)
CO1:	Observe the business decisions with Big data analytics and its applications.	Understand	B	85
CO2:	Apply the analytic process model for the given application through visual data exploration.	Apply	B	85
CO3:	Demonstrate different Analytical models for Predictive analytics.	Analyze	B	85
CO4:	Practice association and sequence rules for transactional data and its applications.	Apply	B	80
CO5:	Examine the performance of survival analysis models with its parametric settings for survival datasets.	Analyze	B	80
CO6:	Investigate the applications of text analytics for real time applications.	Analyze	B	80

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1.	**L**	**L**							**L**		
CO2.	**L**	**L**			**M**				**L**	**L**	
CO3.	**M**	**L**	**L**		**S**			**M**	**M**	**M**	
CO4.	**S**	**M**	**M**	**L**	**S**	**L**		**L**	**M**	**M**	
CO5.	**M**	**M**	**M**		**S**	**L**		**L**	**L**	**M**	
CO6.	**M**	**M**	**M**		**S**	**L**		**L**	**L**	**M**	

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	Continuous			Terminal Examination
	1	2	3	
Remember	30	20	0	0
Understand	30	30	30	30
Apply	20	30	40	40
Analyse	20	20	30	30
Evaluate	0	0	0	0
Create	0	0	0	0

Course Level Assessment Questions

Course Outcome 1 (CO1)**:**

1. List the characteristics of big data.
2. Discuss the variants of NoSQL data models distinguishing it from traditional database.
3. List the major business tools in big data.

Course Outcome 2 (CO2)**:**

1. Identify the requirements of an analytics process model.
2. Describe the Analytics process model?
3. Mention some of the data analytics applications.
4. Suppose that the data for analysis includes the attribute age. The age values for the data tuples are 4, 5, 6, 8, 9, 11, 13, 16, 16 , 18, 20, 21, 25, 30, 31, 33, 36, 37, 40, 41
   Find the mid-range of the data.
   Interpret (roughly) the first quartile (Q1) and the third quartile (Q3) of the data, and give the IQR range.

Course Outcome 3 (CO3)**:**

1. Prepare a predictive model for resource utilization by a computer system which has maximum size of RAM 512 MB, and 120 GB hard disk, which runs 6 processes at a given time with the time allotted for each of the process is about 2 milliseconds.
2. Differentiate among sampling and data pre-processing.
3. Explain in detail about Information retrieval models with data modelling and ranking for a typical IR system describing the logical view of a document.
4. Point out the need for using a multiclass classification model in a system. Clearly provide the reasons over binary classification system with necessary illustrations
5. Depict a predictive model using multiclass classification techniques for any real-time application.
6. Use the data below and perform Pearson Product moment coefficient. Are these two variables positively or negatively correlated?

	Voting Preferences			Row Total
	Republican	Democrat	Independent	
Male	200	150	50	400
Female	250	300	50	600
Column total	450	450	100	1000

Course Outcome 4 (CO4):

1. Take a look at the following table, where *T1*, *T2*, *T3*, *T4*, are the transaction ID's, and *A*, *B*, *C*, *D*, *E* and *K* are the item ID's. The 'database' below has four

transactions. What association rules can be found in this set, if the minimum support (i.e coverage) is 60% and the minimum confidence (i.e. accuracy) is 80%?

Transaction	A	B	C	D	E	K
T1	1	1	0	1	0	1
T2	1	1	1	1	1	0
T3	1	1	1	0	1	0
T4	1	1	0	1	0	0

a. Identify all frequent item set using Apriori Algorithm.
b. List all the strong association rules(with support s and confidence c) matching the following meta-rule, where X is a variable representing customers, and $item_i$ denotes variable representing items (e.g., "A", "B", etc):

   $\forall$ X $\in$ transaction, buys(X, item1) $\wedge$ buys(X, $item_2$) =>buys(X, $item_3$) [s.c]

2. Given the sequence database with the minimum support of 30% and the minimum confidence of 30%, according to the downward closure property.

Value	Data sequence
1	⟨{1}{3}{5}{7, 8, 9}⟩
2	⟨{1}{3}{6}{7, 8}⟩
3	⟨{1, 6}{7}⟩
4	⟨{1} {3} {5, 6}⟩
5	⟨{1}{3}{4}⟩

(i) Choose the support whereby the consequent can appear in any subsequent stage of the sequence.
(ii) Build sequence rules by considering only sessions in which consequent appears right after the antecedent.

3. Demonstrate the relationships between agglomerative, divisive to that of K-means and SOM clustering technique with various schemes used to calculate the distance among the clusters and state your reasons for the distance between the cluster similarities.

Course Outcome 5 (CO5):

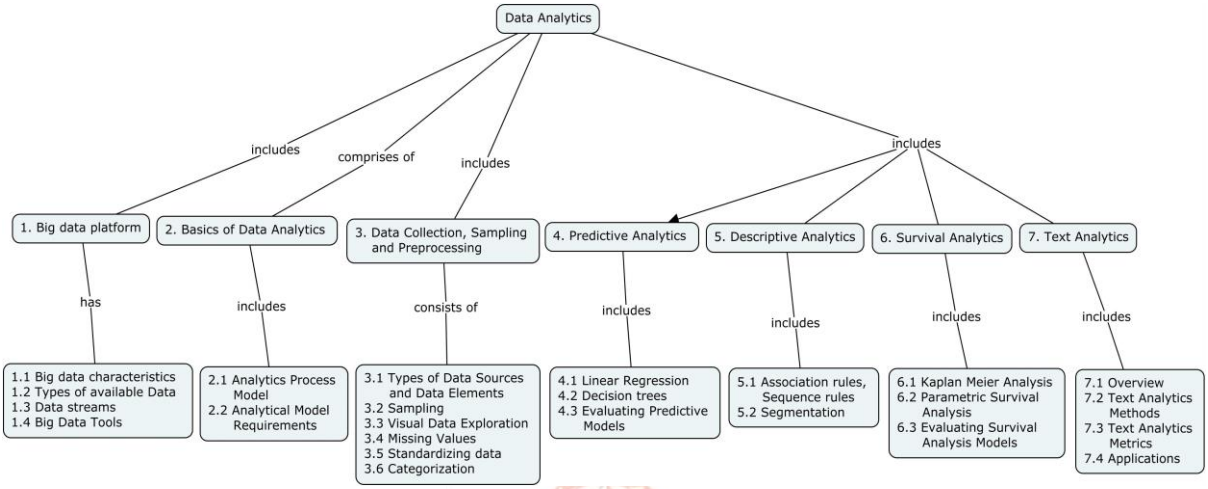
1. Solve the relationship among probability density function F (t), survivor function S (t), and the hazard function H (t), by describing in a mathematically equivalent way of describing a continuous probability distribution.
2. Make use of the following distributions and identify its relationship with respect to the following hazard rate h(t) = f(t)/s(t).
   - Exponential distribution
   - Weibull distribution
   - Maximum likelihood procedures
   - Gamma distribution
3. Illustrate the various data models for parametric survival analytics with event time distribution, compute the various hazard rates. Show the relationship among the models with respect to the hazard rate. $h(t) = \frac{f(t)}{s(t)}$ for the interval $0 \le t \le \infty$.

Course Outcome (CO6):

1. Identify the metrics used for the process of text analytics with respect to its methods and learning techniques.
2. Inspect the various form of identifying subjective material and attitudinal information from a given set of text in text mining process.

3. Examine the sub tasks and components in which a text analysis process must contain and provide justification with reasons in which each of the process relates.

Concept Map



Syllabus

Introduction to Big data platform - Big data characteristics – Types of available Data – Data streams - Big Data Tools

Basics of Data Analytics – Analytics Process Model –Analytical Model Requirements

Data Collection, Sampling and Preprocessing – Types of Data Sources and Data Elements – Sampling – Visual Data Exploration – Missing Values –Standardizing data – Categorization

Predictive Analytics – Linear Regression – Decision trees – Evaluating Predictive Models

Descriptive Analytics – Association rules, sequence rules - segmentation

Survival Analytics – Kaplan Meier Analysis –Parametric Survival Analysis – Evaluating Survival Analysis Models

Text Analytics – Overview – Text Analytics Methods – Text Analytics Metrics – Applications

Reference Books

1. Bart Baesens, “Analytics in a Big Data World”, The Essential Guide to Data Science and its Applications, Wiley, First edition, 2014.
2. Jesus Rogel- Salazar, “Data Science and Analytics with Python “, CRC Press, First Edition, 2017.
3. Michael Berthold, David J. Hand, “Intelligent Data Analysis”, Springer, Second edition, 2007.
4. Thomas H. Davenport, Jeanne G. Harris, “Competing on Analytics: The New Science of Winning”, Harvard Business Review Press ,First edition,2007
5. Paul C. Zikopoulos, Chris Eaton, “Understanding Big Data”, McGraw-Hill, 2012 (eBook from IBM)

6. Chris Eaton, Dirk DeRoos, Tom Deutsch, George Lapis, Paul Zikopoulos, "Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data", McGraw-Hill Publishing, 2012.

Websites

1. https://cognitiveclass.ai/courses/python-for-data-science
2. https://www.edx.org/course/introduction-to-r-for-data-science
3. https://www.edx.org/course/programming-for-data-science
4. https://www.coursera.org/learn/data-analytics-business
5. https://www.coursera.org/learn/text-mining

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1.	**Introduction to Big data platform**	
1.1	Big data characteristics	1
1.2	Types of available Data	1
1.3	Data streams	1
1.4	Big Data Tools	1
2.	**Basics of Data Analytics**	
2.1	Analytics Process Model	2
2.2	Analytical Model Requirements	1
3.	**Data Collection, Sampling and Preprocessing**	
3.1	Types of Data Sources and Data Elements	1
3.2	Sampling	1
3.3	Visual Data Exploration	2
3.4	Missing Values	1
3.5	Standardizing data	1
3.6	Categorization	1
4.	**Predictive Analytics**	
4.1	Linear Regression	1
4.2	Decision trees	1
4.3	Evaluating Predictive Models	1
5.	**Descriptive Analytics**	
5.1	Association rules, Sequence rules	1
5.2	Segmentation	1
6	**Survival Analytics**	
6.1	Kaplan Meier Analysis	1
6.2	Parametric Survival Analysis	1
6.3	Evaluating Survival Analysis Models	1
7.	**Text Analytics**	
7.1	Overview	1
7.2	Text Analytics Methods	1
7.3	Text Analytics Metrics	1
7.4	Applications	1
Total Lectures		**26**

Course Designers:

1. Dr.C.Deisy cdcse@tce.edu
2. A.Sheik Abdullah asait@tce.edu

18PGAA0	PROFESSIONAL AUTHORING

Category	L	T	P	Credit
AC	2	0	0	2

Preamble

On the successful completion of the course, the students will be able to:

1. Explain how to improve your writing skills and level of readability
2. Write each section of research paper
3. Write good quality technical paper

Syllabus

Planning and Preparation, Word Order, Breaking up long sentences, Structuring Paragraphs and Sentences, Being Concise and Removing Redundancy, Avoiding Ambiguity and Vagueness

Clarifying Who Did What, Highlighting Your Findings, Hedging and Criticising, Paraphrasing and Plagiarism, Sections of a Paper, Abstracts. Introduction

Review of the Literature, Methods, Results, Discussion, Conclusions, The Final Check.

Key skills for writing a Title, writing an Abstract, writing an Introduction, writing a Review of the Literature,

Skills for Writing the Methods, Results, Discussion and Conclusions
Useful phrases, how to ensure paper is as good as it could possibly be the first- time submission

Assessment Pattern

Abstract	:	10
Introduction	:	10
Literature Review	:	10
Research Question	:	10
Methods	:	10
Results and Discussion	:	10
Conclusions	:	10
Appropriateness of Title	:	05
Quality of the Paper and Plagiarism	:	25

References

1. Goldbort R, 'Writing for Science', Yale University Press, 2006
2. Day R, 'How to Write and Publish a Scientific Paper', Cambridge University Press, 2006
3. Highman N, 'Handbook of Writing for the Mathematical Sciences, SIAM Highman's book, 1998
4. Adrian Wallwork, 'English for Writing Research Papers', Springer New York Dordrecht Heidelberg London, 2011

18PGAB0	VALUE EDUCATION

Category	L	T	P	Credit
AC	2	0	0	2

Preamble

On the successful completion of the course, the students will be able to:

1. Experience self-development
2. Explain the importance of Human values
3. Develop the overall personality

Syllabus

Values and self-development –Social values and individual attitudes. Work ethics, Indian vision of humanism. Moral and non- moral valuation. Standards and principles, Value judgements

Importance of cultivation of values, Sense of duty. Devotion, Self-reliance. Confidence, Concentration. Truthfulness, Cleanliness, Honesty, Humanity, Power of faith, National Unity, Patriotism, Love for nature, Discipline

Personality and Behavior Development, Soul and Scientific attitude, Positive Thinking. Integrity and discipline, Punctuality, Love and Kindness, Avoid fault Thinking, Free from anger, Dignity of labour, Universal brotherhood and religious tolerance, True friendship, Happiness Vs suffering, love for truth.

Aware of self-destructive habits, Association and Cooperation, Doing best for saving nature

Character and Competence –Holy books vs Blind faith, Self-management and Good health, Science of reincarnation, Equality, Nonviolence , Humility, Role of Women, All religions and same message, Mind your Mind, Self-control, Honesty, Studying effectively

Assessment Pattern

Bloom's Category	Continuous Assessment Test	Terminal Examination
Remember	20	20
Understand	40	40
Apply	40	40
Analyse	0	0
Evaluate	0	0
Create	0	0

References

1. Chakroborty, S.K. "Values and Ethics for organizations Theory and practice", OxforUniversity Press, New Delhi