Program Name : **Computer Engineering Program Group**

Program Code : **CO/CM/IF/CW**

Semester : **Sixth**

Course Title : **Emerging Trends in Computer and Information Technology**

Course Code : **22618**

1. RATIONALE

Advancements and applications of Computer Engineering and Information Technology are ever changing. Emerging trends aims at creating awareness about major trends that will define technological disruption in the upcoming years in the field of Computer Engineering and Information Technology. These are some emerging areas expected to generate revenue, increasing demand as IT professionals and open avenues of entrepreneurship.

2. COMPETENCY

The aim of this course is to help the student to attain the following industry identified competency through various teaching learning experiences:

- **Acquire knowledge of Emerging Trends.**

3. COURSE OUTCOMES (COs)

- Describe machine learning and data concepts.
- Interpret IoT concepts.
- Describe Blockchain technology.
- Describe Digital Forensic Models and Evidence Handling Procedures.
- Describe Ethical Hacking process.
- Detect Network, Operating System, and applications vulnerabilities.

4. TEACHING AND EXAMINATION SCHEME

Teaching Scheme			Credit (L+T+P)	Examination Scheme											
				Theory						Practical					
L	T	P		Paper Hrs.	ESE		PA		Total		ESE		PA		Total	
					Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min
3	--	--	3	90 Min	70*#	28	30*	00	100	40	--	--	--	--	--	--

*(*): Under the theory PA; Out of 30 marks, 10 marks of theory PA are for micro-project assessment to facilitate integration of COs and the remaining 20 marks is the average of 2 tests(**MCQ type**) to be taken during the semester for the assessment of the UOs required for the attainment of the COs.(*#)* :Online Examination

***Legends:* L**-*Lecture;* **T** *– Tutorial/Teacher Guided Theory Practice;* **P** *-Practical;* **C** *– Credit,* **ESE** *-End Semester Examination;* **PA** *- Progressive Assessment.*

5. COURSE MAP (with sample COs, UOs, ADOs and topics)

This course map illustrates an overview of the flow and linkages of the topics at various levels of outcomes (details in subsequent sections) to be attained by the student by the end of the course, in all domains of learning in terms of the industry/employer identified competency depicted at the center of this map.

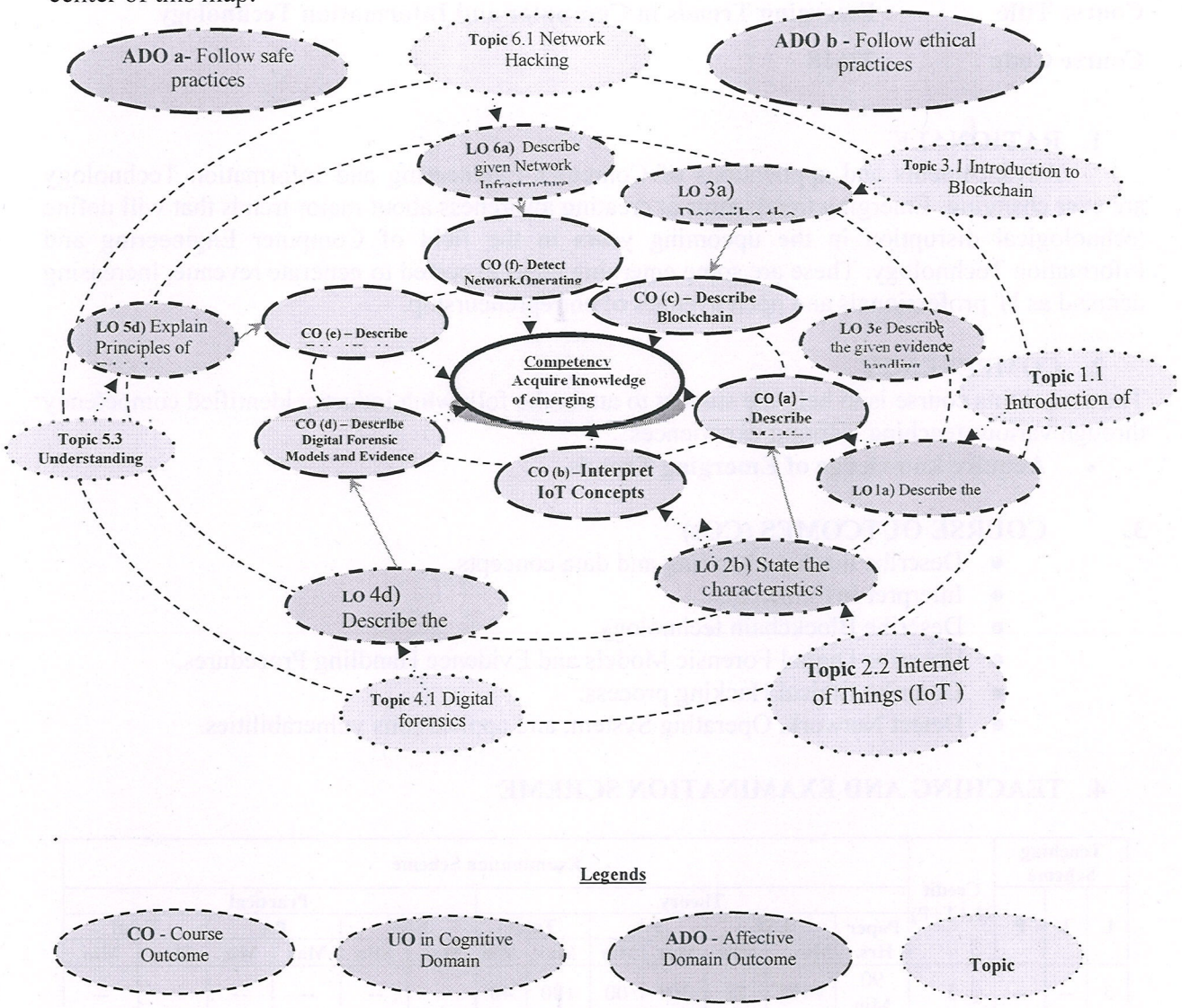

Figure 1 - Course Map

6. SUGGESTED PRACTICALS/ EXERCISES

The practicals in this section are PrOs (i.e. sub-components of the COs) to be developed and assessed in the student for the attainment of the competency.

S. No.	Practical Outcomes (PrOs)	Unit No.	Approx. Hrs. Required
	Not Applicable		

7. MAJOR EQUIPMENT/ INSTRUMENTS REQUIRED

The major equipment with broad specification mentioned here will usher in uniformity in conduct of experiments, as well as aid to procure equipment by authorities concerned.

S. No.	Equipment Name with Broad Specifications	PrO
	Not Applicable	

8. UNDERPINNING THEORY COMPONENTS

Unit	Unit Outcomes (UOs) (in cognitive domain)	Topics and Sub-topics
Unit I : Artificial Intelligence (14 m, 6 hrs)	1a) Describe the concept of AI. 1b) State the components of AI. 1c) List applications of AI 1d) Differentiate between machine learning & deep learning. 1e) Enlist data types of data variables 1f) Describe representation methods of 1g) Describe importance of data storytelling. 1h) Describe exploratory analysis in communication	**1.1 Introduction of AI** • Concept • Scope of AI • Components of AI • Types of AI • Application of AI **1.2 Data Visualization** • **Data types in data visualization** • **Scales map of data values in aesthetics** • **Use of coordinate system in data visualization** • **Use of colors to represent data values** • **Representing - Amounts, Distribution, and Proportions** **1.3 Data Storytelling** • **Introduction** • **Ineffectiveness of Graphical representation of data** • **Explanatory Analysis** ○ **Who** ○ **What** ○ **How** **1.4 Concept of machine learning and deep learning.**
Unit II: Machine to Machine Communication (10m, 10 hrs)	2a) Describe the concept of Embedded System 2b) State the characteristics and features Internet of Thing 2c) Describe the design the IoT 2d) State protocols used in IoT 2e) Compare generations of Mobile	**2.1 Internet of Things (IoT)** • Definition • Characteristics of IoT • Features and Applications of IoT • Advantages and Disadvantages of IoT **2.1.2 Design of IoT** • Physical design of IoT

Unit	Unit Outcomes (UOs) (in cognitive domain)	Topics and Sub-topics
	Network Evaluations. 2f) State characteristics of 5G Network. 2g) Explain NGN Architecture.	• Logical design of IoT **2.1.3 IoT Protocols** **2.1.4 Sensors and actuators used in IoT** **2.2 Introduction to 5G Network** • 5-G characteristics and application areas. • NGN architecture: Features, Functional block diagram, Network components: Media Gateway, Media Gateway Controller, and Application Server. • NGN Wireless Technology: Telecom network Spectrum: Types [licensed and unlicensed], Mobile Network Evolution (2G to 5G), Comparative features, • NGN Core: Features, Multi-Protocol Label Switching (MPLS): Concepts, Features and Advantages.
Unit III : Blockchain Technology	3a) Describe the concept of block-chain 3b) Differentiate between Centralize and Decentralize system 3c) Describe the layers of blockchain. 3d) State the importance of blockchain	**3.1 Introduction to Blockchain** • Backstory of Blockchain • What is Blockchain? **3.2 Centralize versus Decentralized System** **3.3 Layers of Blockchain** • Application Layer • Execution Layer • Semantic Layer • Propagation Layer • Consensus Layer **3.4 Importance of Blockchain** • Limitations of Centralized Systems • Blockchain Adoption So Far **3.5 Blockchain Use and Use Cases**
Unit IV: **Digital Forensics (m- hrs)**	3a. Describe the history of digital forensics 3b. Define digital forensics. 3c. List the rules of digital forensics. 3d. Describe the given model of digital forensic investigation. 3e. State the ethical and unethical	**4.1 Digital forensics** • Introduction to digital forensic • Digital forensics investigation process • Models of Digital Forensic Investigation - o Abstract Digital Forensics

Unit	Unit Outcomes (UOs) (in cognitive domain)	Topics and Sub-topics
	issues in digital forensics. 3f. Define digital evidence. 3g. List the rules of digital evidence. 3h. State characteristics of digital evidence. 3i. Describe the given type of evidence. 3j. Describe the given evidence handling procedures. 3k. Explain Volatile Evidence.	Model (ADFM) o Integrated Digital Investigation Process (IDIP) o An extended model for cybercrime investigation **4.2 Ethical issues in digital forensic** • General ethical norms for investigators • Unethical norms for investigation **4.3 Digital Evidences** • Definition of Digital Evidence • Best evidence rule • Original Evidence **4.4 Characteristics of Digital Evidence** • Locard's Exchange Principle • Digital Stream of bits **4.5 Types of evidence** • Illustrative, Electronics, Documented, Explainable, Substantial, Testimonial **4.6 Challenges in evidence handling** • Authentication of evidence • Chain of custody • Evidence validation **4.7 Volatile evidence**
Unit V: Basics of Hacking (10M- 8Hrs)	5a. Define hackers. 5b. Explain the need to hack your own systems. 5c. Explain the types of attacks a system can face. 5d. Explain Principles of Ethical Hacking. 5e. Describe the Ethical hacking Process.	**5.1 Ethical Hacking** • How Hackers Beget Ethical Hackers • Defining hacker, Malicious users • Data Privacy and General Data Protection and Regulation(GDPR) **5.2 Understanding the need to hack your own systems** **5.3 Understanding the dangers your systems face** • Non Technical attacks • Network-infrastructure attacks • Operating-system attacks • Application and other specialized attacks **5.4 Obeying the Ethical hacking Principles** • Working ethically • Respecting privacy • Not crashing your systems

Unit	Unit Outcomes (UOs) (in cognitive domain)	Topics and Sub-topics
		5.5 The Ethical Hacking Process • Formulating your plan • Selecting tools • Executing the plan • Evaluating results • Moving on **5.6 Cyber Security act**
Unit VI: Types of Hacking (12 M- 10 Hrs)	6a. Describe given Network Infrastructure Vulnerabilities (wired/wireless). 6b. List operating system Vulnerabilities. 6c. Explain Buffer Overflow attack. 6d. Describe given Messaging Systems Vulnerabilities. 6d. Describe given Web Vulnerabilities. 6e. Describe given Database Vulnerabilities.	**6.1 Network Hacking** **Network Infrastructure:** • Network Infrastructure Vulnerabilities • Scanning-Ports • Ping sweep • Scanning SNMP • Grabbing Banners • MAC-daddy attack **Wireless LANs:** • Wireless Network Attacks **6.2 Operating System Hacking** • Introduction of Windows and Linux Vulnerabilities • Buffer Overflow Attack **6.3 Applications Hacking** **Messaging Systems:** • Vulnerabilities • E-Mail Attacks- E-Mail Bombs • Banners • Best practices for minimizing e-mail security risks **Web Applications:** • Web Vulnerabilities • Directories Traversal and Countermeasures • Google Dorking **Database system** • Database Vulnerabilities • Best practices for minimizing database security risks

9. SUGGESTED SPECIFICATION TABLE FOR QUESTION PAPER DESIGN

Unit No.	Unit Title	Teaching Hours	Distribution of Theory Marks			
			R Level	U Level	A Level	Total Marks
I	Artificial Intelligence	08	06	06	--	12

Unit No.	Unit Title	Teaching Hours	Distribution of Theory Marks			
			R Level	U Level	A Level	Total Marks
I	Artificial Intelligence	08	06	06	--	12
II	Machine to Machine communication	08	06	02	02	12
III	Blockchain Technology	08	06	02	02	10
IV	Digital Forensics and Digital Evidences	10	06	06	02	12
V	Basics of Hacking	06	04	06	–	10
VI	Types of Hacking	08	06	06	02	14
	Total	**48**	**34**	**28**	**08**	**70**

Legends: *R=Remember, U=Understand, A=Apply and above (Bloom's Revised taxonomy)*
Note: This specification table provides general guidelines to assist students for their learning and to teachers to teach and assess students with respect to attainment of LOs. The actual distribution of marks at different taxonomy levels (of R, U and A) in the question paper may vary from above table.

10. SUGGESTED STUDENT ACTIVITIES

Other than the classroom learning, following are the suggested student-related ***co-curricular*** activities which can be undertaken to accelerate the attainment of the various outcomes in this course: Students should conduct following activities in group and prepare reports of about 5 pages for each activity, also **collect/record physical evidences for their (student's) portfolio** which will be useful for their placement interviews:

a) Prepare report on suggestive case study of digital forensic, digital evidence and hacking as give below:
   i. The Aaron Caffrey case – United Kingdom, 2003 http://digitalcommons.law.scu.edu/cgi/viewcontent.gi?article=1370&context=chtlj
   ii. The Julie Amero case – Connecticut, 2007 http://dfir.com.br/wp-content/uploads/2014/02/ julieamerosummary.pdf
   iii. The Michael Fiola case – Massachusetts, 2008 http://truthinjustice.org/fiola.htm.
b) Prepare report on any given case study of IoT

11. SUGGESTED SPECIAL INSTRUCTIONAL STRATEGIES (if any)

These are sample strategies, which the teacher can use to accelerate the attainment of the various outcomes in this course:

a) Massive open online courses (***MOOCs***) may be used to teach various topics/subtopics.
b) ***'L' in item No. 4*** does not mean only the traditional lecture method, but different types of teaching methods and media that are to be employed to develop the outcomes.
c) About ***15-20% of the topics/sub-topics*** which is relatively simpler or descriptive in nature is to be given to the students for ***self-directed learning*** and assess the development of the COs through classroom presentations (see implementation guideline for details).
d) With respect to item No.10, teachers need to ensure to create opportunities and provisions for ***co-curricular activities***.
e) Use different Audio Visual media for Concept understanding.
f) Guide student(s) in undertaking micro-projects.

g) Demonstrate students thoroughly before they start doing the practice.
h) Observe continuously and monitor the performance of students.

12. SUGGESTED MICRO-PROJECTS

Only one micro-project is planned to be undertaken by a student that needs to be assigned to him/her in the beginning of the semester. In the first four semesters, the micro-project is group-based. However, in the fifth and sixth semesters, it should be preferably be ***individually*** undertaken to build up the skill and confidence in every student to become problem solver so that s/he contributes to the projects of the industry. In **special situations** where groups have to be formed for micro-projects, the number of students in the group should ***not exceed three.***

The micro-project could be industry application based, internet-based, workshop-based, laboratory-based or field-based. Each micro-project should encompass two or more COs which are in fact, an integration of UOs and ADOs. Each student will have to maintain a dated work diary consisting of individual contributions in the project work and give a seminar presentation of it before submission. The total duration of the micro-project should not be less than ***16 (sixteen) student engagement hours*** during the course. The student ought to submit a micro-project by the end of the semester to develop the industry-oriented COs.

A suggestive list of micro-projects is given here. Similar micro-projects could be added by the concerned faculty:

a) IoT Based Humidity and Temperature Monitoring

i. Explain the need of IoT Based Humidity and Temperature Monitoring.
ii. What will be the hardware requirements for designing this system.
iii. What will be the software requirements
iv. Explain how circuit can be designed for this system along with its working
v. Explain how to design an IoT application and how to store and retrieve a data on it.

b) IoT based Weather Monitoring System

i. Explain the need of IoT Based Weather Monitoring System .
ii. What will be the hardware requirements for designing this system?
iii. What will be the software requirements?
iv. Explain how circuit can be designed for this system along with its working
v. Explain how to design an IoT application and how to store and retrieve a data on it.

c) Study any case of fake profiling. Identify

i. The way digital forensics was used in detecting the fraud.
ii. Where was digital evidence located?
iii. Effects.

d) Study any case of forgery /falsification crime case solved using digital forensics:

i. Identify the model used for Digital Investigation.
ii. Was investigation done ethically or unethically.
iii. Where was digital evidence found for crime establishment?
iv. State the punishment meted.

e) Study Credit card fraud as an identity threat. Identify:

i. Use of digital media in carrying out fraud.

ii. Vulnerability Exploited.
iii. Effect of fraud.
iv. Protection/Precaution to be taken against such frauds.

f) Study any Trojan attack. Identify the Trojan attack:

i. State the way trojan got installed on a particular Machine.
ii. State the effects of the Trojan.
iii. Elaborate/Mention/State protection/Blocking mechanism for this specific Trojan, example specification of any anti-threats platform which filters the Trojan.

g) Case studies related to digital forensics

i. Hosting Obscene profile
ii. Illegal money transfer
iii. Fake travel agent
iv. Creating fake profile

h) Case Study on Blockchain
i. https://research.aimultiple.com/blockchain-case-studies/
ii. https://www.ibm.com/blockchain/use-cases/

13. SUGGESTED LEARNING RESOURCES

S. No.	Title of Book	Author	Publication
1.	Artificial Intelligence	R.B. Mishra	PHI
2.	Introduction to Embedded systems	Shibu K. V	Tata Mcgraw Hill ISBN 978-0-07-014589-4
3.	Beginning Blockchain-A Beginner's Guide to Building Blockchain Solutions	Bikramaditya Singhal Gautam Dhameja Priyanshu Sekhar Panda	Apress, ISBN-13 (pbk): 978-1-4842-3443-3 ISBN-13 (electronic): 978-1-4842-3444-0
4.	Blockchain For Dummies	Tiana Laurence	Wiley India ISBN: 9788126527755
5.	Internet Of Things-A Hands-on Approach	Arshadeep Bahga, Vijay Madisetti,	University Press ISBN 978-8-17371-954-7
6.	The Basics of Digital Forensic	John Sammons	Elsevier ISBN 978-1-59749-661-2
7.	Digital Forensic (2017 Edition)	Dr. Nilakashi Jain Dr. Dhananjat R. Kalbande	Wiley Publishing Inc. ISBN: 978-81-265-6574-0
8.	Hacking for Dummies (5th Edition)	Kevin Beaver CISSP	Wiley Publishing Inc. ISBN: 978-81-265-6554-2
9.	Fundamentals of Data Visualization: A Primer making	Claus O. Wilke	O'Reilly Media Inc. ISBN: 9781492031086

S. No.	Title of Book	Author	Publication
	informative and compelling figures		
10.	Storytelling with data - a data visualization guide for business professionals	cole nussbaumer knaflic	Wiley Publishing Inc. ISBN 9781119002253

SOFTWARE/LEARNING WEBSITES

a) https://www.allitebooks.in/the-internet-of-things/
b) https://www.versatek.com/wp-content/uploads/2016/06/IoT-eBook-version5.pdf
c) https://www.tutorialspoint.com/internet_of_things/internet_of_things_tutorial.pdf
d) http://www.spmkck.co.in/Notes/Learning%20Internet%20of%20Things.pdf
e) https://resources.infosecinstitute.com/digital-forensics-models/#gref.
f) https://www.researchgate.net/publication/300474145_Digital_Forensics/download
g) https://docs.microsoft.com/en-us/sysinternals/downloads/psloggedon
h) www.openwall.com/passwords/windows-pwdump
i) https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_process.htm
j) https://slideplayer.com/slide/7480056/
k) https://www.investopedia.com/terms/b/blockchain.asp
l) https://www.javatpoint.com/blockchain-tutorial
m) https://www.tutorialspoint.com/blockchain/index.htm
n) https://www.guru99.com/blockchain-tutorial.html