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**

4a. 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.

4b. 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.**

4c. COURSE OUTCOMES (COs)

- Describe Artificial Intelligence, Machine learning and deep learning
- Interpret IoT concepts
- Compare Models of Digital Forensic Investigation.
- Describe Evidence Handling procedures.
- Describe Ethical Hacking process.
- Detect Network, Operating System and applications vulnerabilities

4d. 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.*

4e. 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 centre of this map.

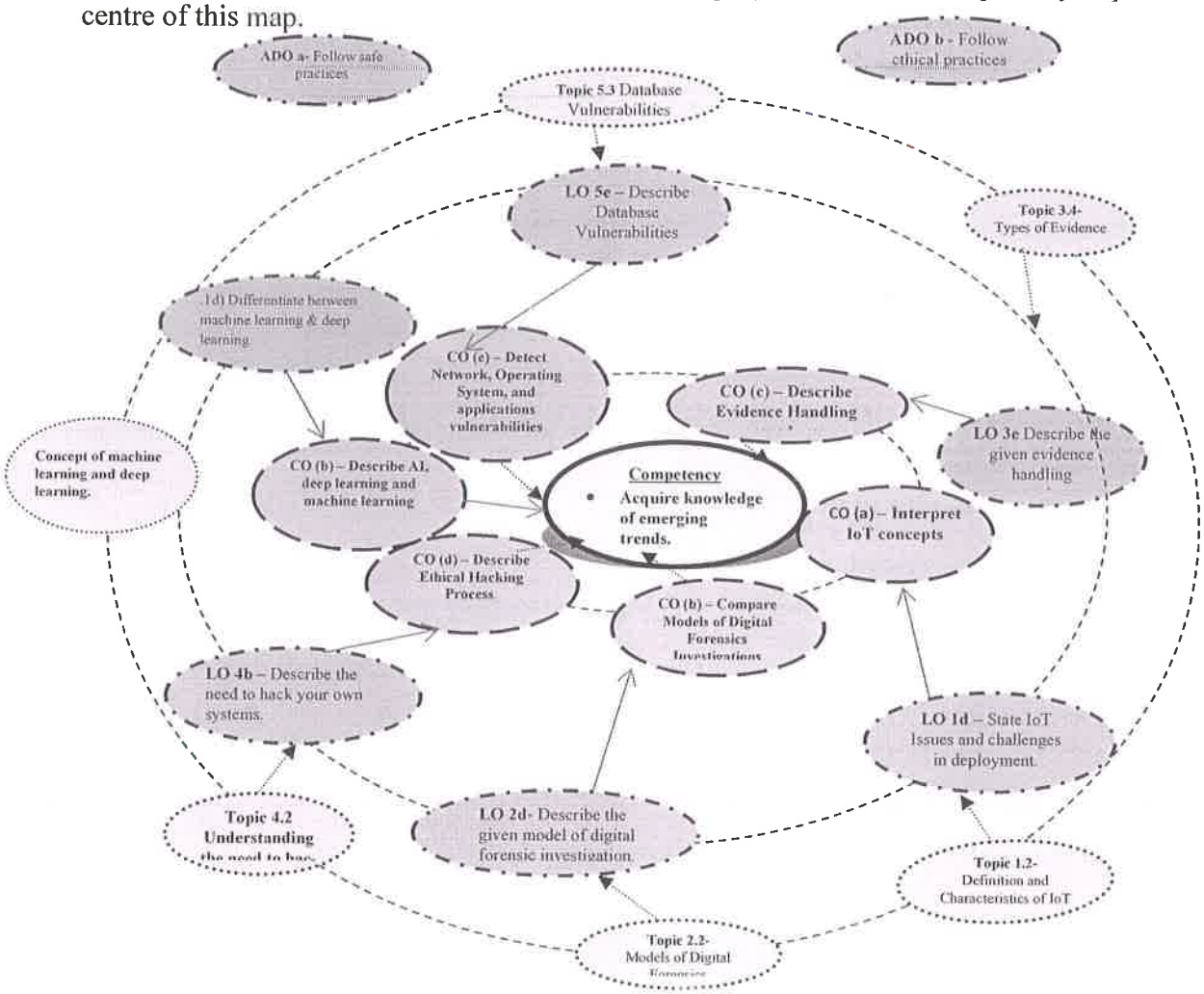

Figure 1 - Course Map

4f. 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		

4g. 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	

4h. UNDERPINNING THEORY COMPONENTS

Unit	Unit Outcomes (UOs) (in cognitive domain)	Topics and Sub-topics
Unit I : Artificial Intelligence (06m, 4 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.	**1.1 Introduction of AI** • Concept • Scope of AI • Components of AI • Types of AI • Application of AI **1.2 Concept of machine learning and deep learning.**
Unit II: Internet of Things (18m,12 hrs)	2a) State the domains and application areas of Embedded Systems 2b) Describe IoT systems in which information and knowledge are inferred from data. 2c) Describe designs of IoT. 2d) State IoT Issues and challenges in deployment.	**2.1 Embedded Systems:** • Embedded system concepts, purpose of Embedded Systems, Architecture of Embedded Systems, Embedded Processors- PIC, ARM, AVR, ASIC **2.2 IoT: Definition and characteristics of IoT** • Physical design of IoT, o Things of IoT o IoT Protocols • Logical design of IoT, o IoT functional blocks, o IoT Communication models, o IoT Communication APIs, • IoT Enabling Technologies • IoT levels and deployment

Unit	Unit Outcomes (UOs) (in cognitive domain)	Topics and Sub-topics
		templates • IoT Issues and Challenges, Applications • IoT Devices and its features: Arduino, Uno, Raspberry Pi, Node Microcontroller Unit
Unit III: Basics of Digital Forensics (8m-5 hrs)	3a. Describe the history of digital forensics 3b. Define digital forensics. 3c. List the rules of digital forensic 3d. Describe the given model of digital forensic investigation. 3e. State the ethical and unethical issues in digital forensics	**3.1 Digital forensics** • Introduction to digital forensic • History of forensic • Rules of digital forensic • Definition of digital forensic • Digital forensics investigation and its goal **3.2 Models of Digital Forensic Investigation** • Digital Forensic Research Workshop Group (DFRWS) Investigative Model • Abstract Digital Forensics Model (ADFM) • Integrated Digital Investigation Process (IDIP) • End to End digital investigation process (EEDIP) • An extended model for cybercrime investigation • UML modeling of digital forensic process model (UMDFPM) **3.3 Ethical issues in digital forensic** • General ethical norms for investigators • Unethical norms for investigation
Unit IV: Digital Evidence (10M- 08 Hrs)	4a. Define digital evidence. 4b. List the rules of digital evidence. 4c. State characteristics of digital evidence. 4d. Describe the given type of evidences 4e. Describe the given evidence handling procedures	**4.1 Digital Evidences** • Definition of Digital Evidence • Best Evidence Rule • Original Evidence **4.2 Rules of Digital Evidence** **4.3 Characteristics of Digital Evidence** • Locard's Exchange Principle • Digital Stream of bits **4.4 Types of evidence** Illustrative, Electronics, Documented, Explainable, Substantial, Testimonial **4.5 Challenges in evidence handling**

Unit	Unit Outcomes (UOs) (in cognitive domain)	Topics and Sub-topics
		• Authentication of evidence • Chain of custody • Evidence validation **4.6 Volatile evidence**
Unit V: Basics of Hacking (12M- 8Hrs)	5a) Define hackers. 5b) Describe the need to hack your own systems. 5c) Describe the dangers in systems. 5d) Describe the Ethical hacking Process 5e) Identify the Hacker's Mindset	**5.1 Ethical Hacking** • How Hackers Beget Ethical Hackers • Defining hacker, Malicious users **5.2 Understanding the need to hack your own systems** **5.3 Understanding the dangers your systems face** • Nontechnical 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 **5.5 The Ethical hacking Process** • Formulating your plan • Selecting tools • Executing the plan • Evaluating results • Moving on **5.6 Cracking the Hacker Mindset** • What You're Up Against? • Who breaks in to computer systems? • Why they do it? • Planning and Performing Attacks • Maintaining Anonymity
Unit VI: Types of Hacking (16 M- 11 Hrs)	6a. Describe Network Infrastructure Vulnerabilities (wired/wireless) 6b. List operating system Vulnerabilities 6c. Describe Messaging Systems Vulnerabilities 6d. Describe Web Vulnerabilities 6e. Describe Database Vulnerabilities	**6.1 Network Hacking** **Network Infrastructure:** • Network Infrastructure Vulnerabilities • Scanning-Ports • Ping sweep • Scanning SNMP • Grabbing Banners • Analysing Network Data and Network Analyzer • MAC-daddy attack

Unit	Unit Outcomes (UOs) (in cognitive domain)	Topics and Sub-topics
		Wireless LANs: • Implications of Wireless Network Vulnerabilities, • Wireless Network Attacks **6.2 Operating System Hacking** • Introduction of Windows and Linux Vulnerabilities **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, **Database system** • Database Vulnerabilities • Best practices for minimizing database security risks

4f. SUGGESTED SPECIFICATION TABLE FOR QUESTION PAPER DESIGN

4g.

Unit No.	Unit Title	Teaching Hours	Distribution of Theory Marks			
			R Level	U Level	A Level	Total Marks
I	Artificial Intelligence (06m,4 hrs)	04	04	02	--	06
II	Internet of Things (18m,12 hrs)	12	10	04	04	18
III	Basics of Digital Forensics (8m-5 hrs)	05	06	02	00	08
IV	Digital Evidence (10M- 08 Hrs)	08	06	02	02	10
V	Basics of Hacking (12M- 08 Hrs)	08	06	04	02	12
VI	Types of Hacking (16 M- 11 Hrs)	11	06	08	02	16
Total		**48**	**38**	**22**	**10**	**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.

4h. 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

4i. 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/sub topics.
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.

4j. 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 dated work diary consisting of individual contribution 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 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 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.

4k. 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.	Internet Of Things-A Hands-on Approach	Arshadeep Bahga, Vijay Madisetti,	University Press ISBN 978-8-17371-954-7
4.	The Basics of Digital Forensic	John Sammons	Elsevier ISBN 978-1-59749-661-2
5.	Digital Forensic (2017 Edition)	Dr. Nilakashi Jain Dr. Dhananjat R. Kalbande	Wiley Publishing Inc. ISBN: 978-81-265-6574-0
6.	Hacking for Dummies (5th Edition)	Kevin Beaver CISSP	Wiley Publishing Inc. ISBN: 978-81-265-6554-2

4l. 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/


MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION MUMBAI